14869K-113000US

# 日 本 国 特 許 庁
## JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

| | |
|---|---|
| 出願年月日<br>Date of Application: | ２００３年１０月　１日 |
| 出願番号<br>Application Number:<br>[ST. 10/C]: | 特願２００３－３４３４８０<br>[ＪＰ２００３－３４３４８０] |
| 出願人<br>Applicant(s): | 株式会社日立製作所 |

２００４年　２月１６日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３００９７６５

【書類名】　特許願
【整理番号】　340301006
【提出日】　平成15年10月 1日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/60
【発明者】
　【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
　【氏名】　諸橋　政幸
【発明者】
　【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
　【氏名】　永井　康彦
【発明者】
　【住所又は居所】　神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　情報・通信グループ内
　【氏名】　相羽　律子
【特許出願人】
　【識別番号】　000005108
　【氏名又は名称】　株式会社日立製作所
【代理人】
　【識別番号】　110000176
　【氏名又は名称】　一色国際特許業務法人
　【代表者】　一色　健輔
【手数料の表示】
　【予納台帳番号】　211868
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1

【書類名】特許請求の範囲
【請求項１】
互いに通信可能な、第一のサイトに設置されている第一の情報処理装置と、第二のサイトに設置されている第二の情報処理装置と、第三のサイトに設置されている第三の情報処理装置と、を備え、
前記第二の情報処理装置は、前記第二のサイトで運用されている情報セキュリティポリシーが対抗できる脅威を示すデータである対策済み脅威データを記憶する対策済み脅威データ記憶部を有し、
前記第三の情報処理装置は、過去に生じた脅威を示すデータである脅威データを記憶する脅威データ記憶部を有し、
前記第二の情報処理装置は、前記対策済み脅威データを前記第一の情報処理装置に送信する対策済み脅威データ送信部を有し、
前記第三の情報処理装置は、前記脅威データを前記第一の情報処理装置に送信する脅威データ送信部を有し、
前記第一の情報処理装置は、前記対策済み脅威データを受信する対策済み脅威データ受信部と、前記脅威データを受信する脅威データ受信部とを有し、
前記第一の情報処理装置は、前記脅威データと、前記対策済み脅威データとの対応を示すデータである対応データを記憶する対応データ記憶部を有し、
前記第一の情報処理装置は、前記対応データに基づいて、前記対策済み脅威データ受信部が受信した前記対策済み脅威データの中から、前記脅威データ受信部が受信した脅威データに、対応する脅威データが存在するものを抽出する有効な対策済み脅威データ抽出部と、抽出した前記対策済み脅威データを記載した評価データを生成する評価データ生成部とを有すること、
を特徴とする情報セキュリティポリシー評価システム。
【請求項２】
互いに通信可能な、第一のサイトに設置されている第一の情報処理装置と、第二のサイトに設置されている第二の情報処理装置と、第三のサイトに設置されている第三の情報処理装置と、を備え、
前記第二の情報処理装置は、前記第二のサイトで運用されている情報セキュリティポリシーが対抗できる脅威を示すデータである対策済み脅威データを記憶する対策済み脅威データ記憶部を有し、
前記第三の情報処理装置は、過去に生じた脅威を示すデータである脅威データを記憶する脅威データ記憶部を有し、
前記第二の情報処理装置は、前記対策済み脅威データを前記第一の情報処理装置に送信する対策済み脅威データ送信部を有し、
前記第三の情報処理装置は、前記脅威データを前記第一の情報処理装置に送信する脅威データ送信部を有し、
前記第一の情報処理装置は、前記対策済み脅威データを受信する対策済み脅威データ受信部と、前記脅威データを受信する脅威データ受信部とを有し、
前記第一の情報処理装置は、前記脅威データと、前記対策済み脅威データとの対応を示すデータである対応データを記憶する対応データ記憶部を有し、
前記第一の情報処理装置は、前記対応データに基づいて、前記脅威データ受信部が受信した前記脅威データの中から、対応する対策済み脅威データが、前記対策済み脅威データ受信部が受信した前記対策済み脅威データ中に存在しない脅威データを抽出する未対策脅威データ抽出部と、抽出した脅威データを記載した評価データを生成する評価データ生成部とを有すること、
を特徴とする情報セキュリティポリシー評価システム。
【請求項３】
請求項１に記載の情報セキュリティポリシー評価システムにおいて、
前記第一の情報処理装置は、

前記脅威データのそれぞれについて、その脅威により被害を受けた場合に生じる損害の大きさを示すデータである損害量データを記憶する損害量データ記憶部を有し、
前記評価データ生成部は、前記有効な対策済み脅威データ抽出部により抽出した前記対策済み脅威データを、前記各対策済み脅威データについて前記対応データに対応づけられている前記脅威データの前記損害量データの降順に整列して記載した前記評価データを生成する効果順整列部を有すること、
を特徴とする情報セキュリティポリシー評価システム。
【請求項４】
請求項１に記載の情報セキュリティポリシー評価システムにおいて、
前記第一の情報処理装置は、
前記脅威データのそれぞれについて、その脅威により被害を受けた場合に生じる損害の大きさを示すデータである損害量データを記憶する損害量データ記憶部を有し、
前記評価データ生成部は、前記未対策脅威データ抽出部により抽出された前記脅威データを、前記損害量データの降順に整列して記載した前記評価データを生成する考慮優先順整列部を有すること、
を特徴とする情報セキュリティポリシー評価システム。
【請求項５】
請求項３または４に記載の情報セキュリティポリシー評価システムにおいて、
前記第三の情報処理装置の前記脅威データ送信部は、前記損害量データを前記脅威データに付帯させて前記第一の情報処理装置に送信し、
前記第一の情報処理装置の前記脅威データ受信部は、前記脅威データとともに前記損害量データを受信し、
前記第一の情報処理装置の前記損害量データ記憶部は、受信した前記損害量データを記憶すること、
を特徴とする情報セキュリティポリシー評価システム。
【請求項６】
請求項１～４のいずれかに記載の情報セキュリティポリシー評価システムにおいて、前記第三の情報処理装置は、前記脅威データを更新する脅威データ更新部を有し、前記脅威データ送信部は、前記脅威データ更新部により前記脅威データが更新された場合に前記更新後の脅威データを前記第一の情報処理装置に送信すること、
を特徴とする情報セキュリティポリシー評価システム。
【請求項７】
請求項１～４のいずれかに記載の情報セキュリティポリシー評価システムにおいて、前記評価データ生成部により生成された評価データの内容をディスプレイに表示もしくは印刷装置により印字する評価結果出力部を有すること、
を特徴とする情報セキュリティポリシー評価システム。
【請求項８】
請求項１～４のいずれかに記載の情報セキュリティポリシー評価システムにおいて、
前記第一乃至第三の情報処理装置と通信可能に接続している、第四のサイトに設置されている第四の情報処理装置を備え、
前記第四の情報処理装置は、前記第二のサイトを運営する組織が加入している、脅威による被害を受けた場合に生じる損害を補償する保険の補償額を記憶する補償額記憶部を有し、
前記第一の情報処理装置は、前記評価データ生成部により生成された前記評価データを、前記第四の情報処理装置に送信する評価データ送信部を有し、
前記第四の情報処理装置は、前記評価データを受信する評価データ受信部を有し、
前記第四の情報処理装置は、記憶している前記補償額を、前記評価データ受信部により受信した前記評価データに応じて決定される前記補償額に設定し直す補償額設定部を有すること、
を特徴とする情報セキュリティポリシー評価システム。

【請求項９】
請求項１～４のいずれかに記載の情報セキュリティポリシー評価システムにおいて、
前記第二のサイトは情報セキュリティポリシーの評価を依頼する顧客のサイトであり、前記第三のサイトは、脅威に関する情報を収集しその提供を行っている脅威情報を提供する脅威情報提供業者のサイトであり、前記第一のサイトは、前記顧客からの依頼に応じて前記第二のサイトで運用されている情報セキュリティポリシーの評価を行う評価業者のサイトであること、
を特徴とする情報セキュリティポリシー評価システム。
【請求項１０】
請求項８に記載の情報セキュリティポリシー評価システムにおいて、
前記第二のサイトは情報セキュリティポリシーの評価を依頼する顧客のサイトであり、
前記第三のサイトは、脅威に関する情報を収集しその提供を行っている脅威情報を提供する脅威情報提供業者のサイトであり、
前記第一のサイトは、前記顧客からの依頼に応じて前記第二のサイトで運用されている情報セキュリティポリシーの評価を行う評価業者のサイトであり、
前記第四のサイトは、前記顧客を加入者とし、前記第二のサイトが脅威を受けた場合に生じる損害を補償する保険を商品とする保険業を運営する保険業者のサイトであり、
前記顧客は、前記評価業者に前記情報セキュリティポリシーの評価を依頼するための評価手数料を支払い、
前記評価業者は、前記顧客から前記評価手数料を受け取り、
前記評価業者は、受け取った前記評価手数料の一部を情報提供料として前記脅威情報提供業者に支払い、
前記評価業者は、受け取った前記評価手数料の一部を前記補償額を変更するかわりに前記保険業者に支払い、
前記顧客が前記保険のために支払う保険料として支払い、
前記保険業者は、前記評価データに応じて前記補償額を決定すること、
を特徴とする情報セキュリティポリシー評価システム。
【請求項１１】
請求項１０に記載の情報セキュリティポリシー評価システムにおいて、
前記評価業者もしくは前記保険業者は、前記顧客が、前記情報セキュリティポリシーに従って適切に運用を行っているかどうかを監査した監査レポートを作成し、前記監査レポートに応じて前記補償額を決定すること、
を特徴とする情報セキュリティポリシー評価システム。
【請求項１２】
請求項８に記載の情報セキュリティポリシー評価システムにおいて、
前記第四の情報処理装置は、前記第一のサイトに設置され、前記第一の情報処理装置を運営する組織と同じ組織によって運営されていること、
を特徴とする情報セキュリティポリシー評価システム。
【請求項１３】
互いに通信可能な、第一のサイトに設置されている第一の情報処理装置と、第二のサイトに設置されている第二の情報処理装置と、第三のサイトに設置されている第三の情報処理装置と、を備え、
前記第二の情報処理装置は、前記第二のサイトで運用されている情報セキュリティポリシーを示すデータであるポリシーデータを記憶するポリシーデータ記憶部を有し、
前記第三の情報処理装置は、過去に生じた脅威を示すデータである脅威データを記憶する脅威データ記憶部を有し、
前記第二の情報処理装置は、前記ポリシーデータを前記第一の情報処理装置に送信するポリシーデータ送信部を有し、
前記第三の情報処理装置は、前記脅威データを前記第一の情報処理装置に送信する脅威データ送信部を有し、

前記第一の情報処理装置は、前記ポリシーデータを受信するポリシーデータ受信部と、前記脅威データを受信する脅威データ受信部とを有し、
前記第一の情報処理装置は、前記脅威データと、前記脅威データが示す脅威に対して有効な情報セキュリティポリシーを示すポリシーデータとの対応を示すデータである対応データを記憶する対応データ記憶部を有し、
前記第一の情報処理装置は、前記対応データに基づいて、前記ポリシーデータ受信部が受信した前記ポリシーデータの中から、前記脅威データ受信部が受信した脅威データに、対応する脅威データが存在するポリシーデータを抽出する有効なポリシーデータ抽出部と、抽出した前記ポリシーデータを記載した評価データを生成する評価データ生成部とを有すること、
を特徴とする情報セキュリティポリシー評価システム。
【請求項１４】
互いに通信可能な、第一のサイトに設置されている第一の情報処理装置と、第二のサイトに設置されている第二の情報処理装置と、第三のサイトに設置されている第三の情報処理装置と、を備え、
前記第二の情報処理装置は、前記第二のサイトで運用されている情報セキュリティポリシーを示すデータであるポリシーデータを記憶するポリシーデータ記憶部を有し、
前記第三の情報処理装置は、過去に生じた脅威を示すデータである脅威データを記憶する脅威データ記憶部を有し、
前記第二の情報処理装置は、前記ポリシーデータを前記第一の情報処理装置に送信するポリシーデータ送信部を有し、
前記第三の情報処理装置は、前記脅威データを前記第一の情報処理装置に送信する脅威データ送信部を有し、
前記第一の情報処理装置は、前記ポリシーデータを受信するポリシーデータ受信部と、前記脅威データを受信する脅威データ受信部とを有し、
前記第一の情報処理装置は、前記脅威データと、前記脅威データが示す脅威に対して有効な情報セキュリティポリシーを示すポリシーデータとの対応を示すデータである対応データを記憶する対応データ記憶部を有し、
前記第一の情報処理装置は、前記対応データに基づいて、前記脅威データ受信部が受信した前記脅威データの中から、前記ポリシーデータ受信部が受信した前記ポリシーデータ中に、対応するポリシーデータが存在しない脅威データを抽出する未対策脅威データ抽出部と、抽出した脅威データを記載した評価データを生成する評価データ生成部とを有すること、
を特徴とする情報セキュリティポリシー評価システム。
【請求項１５】
互いに通信可能な、第一のサイトに設置されている第一の情報処理装置と、第二のサイトに設置されている第二の情報処理装置と、第三のサイトに設置されている第三の情報処理装置と、を備える情報セキュリティポリシー評価システムの制御方法であって、
前記第二の情報処理装置は、前記第二のサイトで運用されている情報セキュリティポリシーが対抗できる脅威を示すデータである対策済み脅威データを記憶し、
前記第三の情報処理装置は、過去に生じた脅威を示すデータである脅威データを記憶し、
前記第二の情報処理装置は、前記対策済み脅威データを前記第一の情報処理装置に送信し、
前記第三の情報処理装置は、前記脅威データを前記第一の情報処理装置に送信し、
前記第一の情報処理装置は、前記対策済み脅威データ及び前記脅威データを受信し、
前記第一の情報処理装置は、前記脅威データと、前記対策済み脅威データとの対応を示すデータである対応データを記憶し、
前記第一の情報処理装置は、前記対応データに基づいて、前記対策済み脅威データ受信部が受信した前記対策済み脅威データの中から、前記脅威データ受信部が受信した脅威デ

ータに、対応する脅威データが存在するものを抽出する有効な対策済み脅威データ抽出部と、抽出された前記対策済み脅威データを記載した評価データを生成すること、
を特徴とする情報セキュリティポリシー評価システムの制御方法。
【請求項１６】
互いに通信可能な、第一のサイトに設置されている第一の情報処理装置と、第二のサイトに設置されている第二の情報処理装置と、第三のサイトに設置されている第三の情報処理装置と、を備える情報セキュリティポリシー評価システムの制御方法であって、
前記第二の情報処理装置は、前記第二のサイトで運用されている情報セキュリティポリシーが対抗できる脅威を示すデータである対策済み脅威データを記憶し、
前記第三の情報処理装置は、過去に生じた脅威を示すデータである脅威データを記憶し、
前記第二の情報処理装置は、前記対策済み脅威データを前記第一の情報処理装置に送信し、
前記第三の情報処理装置は、前記脅威データを前記第一の情報処理装置に送信し、
前記第一の情報処理装置は、前記対策済み脅威データ及び前記脅威データを受信し、
前記第一の情報処理装置は、前記脅威データと、前記対策済み脅威データとの対応を示すデータである対応データを記憶し、
前記対応データに基づいて、前記脅威データ受信部が受信した前記脅威データの中から、対応する対策済み脅威データが、前記対策済み脅威データ受信部が受信した前記対策済み脅威データ中に存在しない脅威データを抽出し、抽出した脅威データを記載した評価データを生成すること、
を特徴とする情報セキュリティポリシー評価システムの制御方法。

【書類名】明細書
【発明の名称】情報セキュリティポリシー評価システム及びその制御方法
【技術分野】
【０００１】
この発明は、情報セキュリティポリシー評価システム及びその制御方法に関し、特に企業等の組織において企業等の組織において情報セキュリティポリシーを効率よくかつ適切に策定し運用する技術に関する。
【背景技術】
【０００２】
ＩＴ関連産業の発達に伴い、情報処理システムに対する脅威が問題となっている。企業等の組織においては、これら脅威に対する対策が進められている。ＢＳ７７９９（英国の情報セキュリティマネジメント規格）に準拠した情報セキュリティマネジメントを推進する組織も増えつつある。ＪＩＰＤＥＣ（日本情報処理開発協会）が推進するＩＳＭＳ（情報セキュリティマネジメントシステム）適合性評価制度等も注目されており、多くの組織において情報セキュリティポリシーが策定され運用されるようになってきている。
【特許文献１】特開２００２－２８８３７１号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】
企業等の組織において策定され運用されている情報セキュリティポリシーは、策定時に把握される情報に基づいて有効性が判断されている。そのため、既に策定され運用されている情報セキュリティポリシーが、必ずしも将来的に有効であるかどうかはわからない。情報処理システムに影響を与える脅威の種類や内容は、技術の進歩や情報処理システムを取り巻く物理的、人的な環境変化に伴って時事刻々と変化していくからである。従って、企業等の組織は、策定され運用されている情報セキュリティポリシーの妥当性について、随時評価や見直しを行っていかなければならない。ここでこのような評価や見直しを適切に行っていくためには、通信ネットワーク上で過去に発生した不正アクセスに関する情報等、脅威に関する情報収集を行う必要があり、情報セキュリティに関する豊富な知識や経験も要求される。
【０００４】
しかしながら、企業等の組織が自ら脅威に関する情報の収集を行い、評価や見直しを行うために必要となる技術レベルを維持していくことは、組織にとって多大な負担である。また、企業等の組織が自身で評価や見直しを行う場合、客観性が損なわれて適切な判断がされなくなる可能性もある。
【０００５】
特許文献１には、機械設備のユーザが、機械設備の保全次第で保守料及び保険料の支払いを削減でき、メーカーは保守費の支払いを、保険会社は保険金支払いを低減できる保守料及び保険料の設定システムが記載されている。この技術では、保全評価システムが通信回線を経由して機械設備に関する保全情報を取得して、保守契約と保全情報とに基づいて保守料を決定している。ここで情報セキュリティポリシーの妥当性の評価や見直しを行うためには、既に実施されている対策の有効性と不足している対策を把握する必要があるが、特許文献１に記載の技術では、不足している対策を把握することはできても既に実施されている対策の価値や有効性はわからない。
【０００６】
本発明はこのような背景に鑑みてなされたものであり、企業等の組織において情報セキュリティポリシーを効率よくかつ適切に策定し運用することができる情報セキュリティポリシー評価システムを提供することを目的とする。
【課題を解決するための手段】
【０００７】
上記目的を達成するための本発明のうちの主たる発明の一つは、情報セキュリティポリ

シー評価システムであって、互いに通信可能な、第一のサイトに設置されている第一の情報処理装置と、第二のサイトに設置されている第二の情報処理装置と、第三のサイトに設置されている第三の情報処理装置と、を備え、前記第二の情報処理装置は、前記第二のサイトで運用されている情報セキュリティポリシーが対抗できる脅威を示すデータである対策済み脅威データを記憶する対策済み脅威データ記憶部を有し、前記第三の情報処理装置は、過去に生じた脅威を示すデータである脅威データを記憶する脅威データ記憶部を有し、　前記第二の情報処理装置は、前記対策済み脅威データを前記第一の情報処理装置に送信する対策済み脅威データ送信部を有し、前記第三の情報処理装置は、前記脅威データを前記第一の情報処理装置に送信する脅威データ送信部を有し、前記第一の情報処理装置は、前記対策済み脅威データを受信する対策済み脅威データ受信部と、前記脅威データを受信する脅威データ受信部とを有し、前記第一の情報処理装置は、前記脅威データと、前記対策済み脅威データとの対応を示すデータである対応データを記憶する対応データ記憶部を有し、前記第一の情報処理装置は、前記対応データに基づいて、前記対策済み脅威データ受信部が受信した前記対策済み脅威データの中から、前記脅威データ受信部が受信した脅威データに、対応する脅威データが存在するものを抽出する有効な対策済み脅威データ抽出部と、抽出した前記対策済み脅威データを記載した評価データを生成する評価データ生成部とを有することとする。

【０００８】

上記第二のサイトは、例えば、情報セキュリティポリシーの評価を依頼する顧客のサイトである。上記第三のサイトは、例えば、脅威に関する情報を収集しその提供を行っている脅威情報を提供する脅威情報提供業者のサイトである。上記第一のサイトは、例えば、前記顧客からの依頼に応じて前記第二のサイトで運用されている情報セキュリティポリシーの評価を行う評価業者のサイトである。

【０００９】

本発明によれば、第一の情報処理装置が、前記対応データに基づいて、前記対策済み脅威データ受信部が受信した前記対策済み脅威データの中から、対応する脅威データが前記脅威データ受信部が受信した脅威データに存在する対策済み脅威データを抽出し、抽出された前記対策済み脅威データを記載した評価データを生成する。ここでこの評価データに記載されている対策済み脅威データが示す情報セキュリティポリシーは、実際に生じた脅威に対して有効であった情報セキュリティポリシーである。従って、評価データに基づいて、第二のサイトにおいて策定され運用されている情報セキュリティポリシーの妥当性を評価することができる。このように第一のサイトにおいて第二のサイトにおける情報セキュリティポリシーの妥当性を示す評価データが作成されることで、第二のサイトを運営する企業等の組織は、自らが策定し運用を行っている情報セキュリティポリシーの評価や見直しのために、自ら脅威に関する情報の収集を行う必要がなく、また、情報セキュリティポリシーの評価や見直しを行うために必要とされる技術水準を維持するための管理負担から開放される。従って、第二のサイトを運営する組織では、情報セキュリティポリシーの評価や見直しを効率よく行うことができる。また発明の評価レポートは単に未対策の脅威を指摘したレポートとは異なり、既に運用されている情報セキュリティポリシーの効果、価値、有効性等についての評価を記載したものである。従って、評価レポートは、経営層（社長、情報セキュリティ担当役員などの上位経営管理者等）や組織のメンバー（従業員等）に情報セキュリティポリシーの効果、価値、有効性等を理解させ遵守させる動機付けとなる有用な資料となり、評価レポートを活用することにより組織における情報セキュリティマネジメントの円滑的な運用が促進されることとなる。また、情報セキュリティポリシーの評価や見直しが第三の情報処理装置から送信されてくる過去に生じた脅威を示すデータに基づいて行われるため、客観的な評価が行われることになり、第二のサイトにおいて策定され運用されている情報セキュリティポリシーについての適切な評価や見直しを行うことが可能となる。

【００１０】

本発明のうちの主たる発明の一つは、情報セキュリティポリシー評価システムであって

、互いに通信可能な、第一のサイトに設置されている第一の情報処理装置と、第二のサイトに設置されている第二の情報処理装置と、第三のサイトに設置されている第三の情報処理装置と、を備え、前記第二の情報処理装置は、前記第二のサイトで運用されている情報セキュリティポリシーが対抗できる脅威を示すデータである対策済み脅威データを記憶する対策済み脅威データ記憶部を有し、前記第三の情報処理装置は、過去に生じた脅威を示すデータである脅威データを記憶する脅威データ記憶部を有し、前記第二の情報処理装置は、前記対策済み脅威データを前記第一の情報処理装置に送信する対策済み脅威データ送信部を有し、前記第三の情報処理装置は、前記脅威データを前記第一の情報処理装置に送信する脅威データ送信部を有し、前記第一の情報処理装置は、前記対策済み脅威データを受信する対策済み脅威データ受信部と、前記脅威データを受信する脅威データ受信部とを有し、　前記第一の情報処理装置は、前記脅威データと、前記対策済み脅威データとの対応を示すデータである対応データを記憶する対応データ記憶部を有し、前記第一の情報処理装置は、前記対応データに基づいて、前記脅威データ受信部が受信した前記脅威データの中から、対応する対策済み脅威データが、前記対策済み脅威データ受信部が受信した前記対策済み脅威データ中に存在しない脅威データを抽出する未対策脅威データ抽出部と、抽出した脅威データを記載した評価データを生成する評価データ生成部とを有することとする。

【００１１】

本発明によれば、第一の情報処理装置が、前記脅威データ受信部が受信した前記脅威データの中から、対応する対策済み脅威データが、前記対応データに基づいて、前記対策済み脅威データ受信部が受信した前記対策済み脅威データ中に存在しない脅威データを抽出し、抽出した脅威データを記載した評価データを生成する。

【００１２】

ここでこの評価データに記載されている脅威データが示す脅威は、実際に生じた脅威であって、その脅威に対し第二のサイトでは何ら有効な情報セキュリティポリシーが運用されていなかった脅威である。従って、この評価データは、例えば、第二のサイトでは、次回の情報セキュリティポリシーの改訂時に優先的に対策を講ずるべき脅威を示した情報として利用される。このように第二のサイトにおいて不足している情報セキュリティポリシーを示した評価データが第一のサイトにおいて自動的に作成されることで、第二のサイトを運営する企業等の組織は、自らが策定し運用を行っている情報セキュリティポリシーの評価や見直しのために、自ら脅威に関する情報の収集を行う必要がなく、また、情報セキュリティポリシーの評価や見直しを行うために必要とされる技術水準を維持するための管理負担から開放される。従って、第二のサイトを運営する組織では、情報セキュリティポリシーの評価や見直しを効率よく行うことができる。また発明の評価レポートは単に未対策の脅威を指摘したレポートとは異なり、既に運用されている情報セキュリティポリシーの効果、価値、有効性等についての評価を記載したものである。従って、評価レポートは、経営層（社長、情報セキュリティ担当役員などの上位経営管理者等）や組織のメンバー（従業員等）に情報セキュリティポリシーの効果、価値、有効性等を理解させ遵守させる動機付けとなる有用な資料となり、評価レポートを活用することにより組織における情報セキュリティマネジメントの円滑的な運用が促進されることとなる。また、情報セキュリティポリシーの評価や見直しが第三の情報処理装置から送信されてくる過去に生じた脅威を示すデータに基づいて行われるため、客観的な評価が行われることになり、第二のサイトにおいて策定され運用されている情報セキュリティポリシーについての適切な評価や見直しを行うことが可能となる。

【発明の効果】

【００１３】

本発明によれば、企業等の組織における情報セキュリティポリシーの策定及び運用を効率よく適切に行うことが可能となる。

【発明を実施するための最良の形態】

【００１４】

以下、本発明の実施例につき図面とともに詳細に説明する。

【００１５】

＝＝＝第一実施例＝＝＝

図１に本発明の第一実施例として説明する情報セキュリティポリシー評価システム（以後、ポリシー評価システムとも称する）の概略構成を示している。この図において、第一のサイト１０１は、顧客からの依頼に応じて第二のサイト１０２で運用されている情報セキュリティポリシーの評価を行う評価業者のサイトである。第二のサイト１０２は、情報セキュリティポリシーの評価を前記評価業者に依頼する前記顧客のサイトである。第三のサイト１０３は、脅威に関する情報を収集しその提供を行っている脅威情報を提供する脅威情報提供業者のサイトである。脅威情報提供業者は、不正アクセス等の情報提供元であり、例えば、ＪＰＣＥＲＴ／ＣＣ（JaPan Computer Emergency Response Team/Coordination Center）や報道／ニュースなどのメディアセンター等は脅威情報提供業者となりうる。

【００１６】

第一のサイト１０１には第一の情報処理装置１１１が設けられている。第二のサイト１０２には第二の情報処理装置１１２が設けられている。第三のサイト１０３には第三の情報処理装置１１３が設けられている。第一乃至第三の情報処理装置１１１，１１２，１１３はそれぞれインターネットや専用線等の通信ネットワーク５０に接続しており、第一乃至第三の情報処理装置１１１，１１２，１１３は通信ネットワーク５０を介して互いに通信可能に接続されている。第一乃至第三の情報処理装置１１１，１１２，１１３としては、パーソナルコンピュータやオフコン、メインフレーム等のコンピュータが用いられる。

【００１７】

本実施例におけるポリシー評価システムの評価対象となる情報セキュリティポリシーについて説明する。情報セキュリティポリシーとは、企業等の組織において、組織が保有する情報資産を保護するために、情報システムの機密性、完全性、可用性等を確保するための情報セキュリティに対する基本方針や対策基準等を定めたものをいう。ＩＴ社会の進展に伴い、情報セキュリティポリシーを策定し運用することは企業等の組織における社会的義務となっている。昨今では、妥当な情報セキュリティポリシーを策定していない組織はＢtoＢ等のオープンな取引市場に参加できないことも多くなってきている。情報セキュリティポリシーは、具体的には階層的に記述された文書として表現される。情報セキュリティポリシーの一例として、外部ネットワーク接続に関する情報セキュリティについての基本方針を例示する。この基本方針は、例えば、インターネット利用に関する標準、外部公開に関する標準、専用線およびＶＰＮ接続に関する標準、リモートアクセスに関する標準、ウイルス対策に関する標準、顧客のプライバシーに関する標準、情報セキュリティ教育に関する標準、罰則に関する標準、スタンダード更新手順に関する標準等を含んでいる。また、上記インターネット利用に関する標準は、例えば、電子メール利用に関する標準、Ｗｅｂの利用に関する標準、アカウント管理に関する標準等を含んでいる。さらに、上記電子メール利用に関する標準には、社内の電子メールを社外のメールサーバへ転送してはならない、機密情報を社外へ送信してはならない、不用意にメールアカウントを外部へ公開してはならない、電子メールの添付ファイルにウイルスが内在することの可能性を考慮しなければならないといった基準を含んでいる。

【００１８】

図２に第一乃至第三の情報処理装置１１１，１１２，１１３として用いられるコンピュータの典型的なハードウエア構成を示している。ＣＰＵ２０１は、情報処理装置の制御を司るもので、ＲＡＭ・ＲＯＭ等のメモリ２０２や記憶装置２０８に格納されたプログラム２０２ｃを実行することにより各種の機能等を実現する。記録媒体読取装置２０４は、記録媒体２０７に記録されているプログラムやデータを読み取るための装置である。読み取られたプログラムやデータは、メモリ２０２もしくは記憶装置２０８に格納される。従って、例えば、記録媒体２０７に記録されたプログラム２０２ｃを、記録媒体読取装置２０４を用いて上記記録媒体２０７から読み取って、メモリ２０２や記憶装置２０８に格納す

るようにすることができる。例えば、上述のデータベースに記憶されるデータは、メモリ２０２もしくは記憶装置２０８に格納される。記録媒体２０７としてはフレキシブルディスクやＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、半導体メモリ等を用いることができる。

【００１９】

記録媒体読取装置２０４は、コンピュータ２００に内蔵されている形態とすることもできるし、外付されている形態とすることもできる。記憶装置２０８は、例えばハードディスク装置やフレキシブルディスク装置、半導体記憶装置等である。入力装置２０５は、オペレータ等によるコンピュータ２００へのデータ入力等のために用いられる。入力装置２０５としては、例えば、キーボードやマウス等が用いられる。出力装置２０６は、情報を外部に出力するための装置である。出力装置２０６としては、例えば、ディスプレイやプリンタ等が用いられる。通信インタフェース２０３は、コンピュータ２００を通信ネットワークに接続するためのインタフェースである。コンピュータ２００は、通信インタフェース２０３を介して他のコンピュータ等の外部装置との間で通信を行うことができる。なお、第一乃至第三の情報処理装置１１１，１１２，１１３は、以上に説明したハードウエアの全てを必ずしも備えている必要はない。

【００２０】

次に、第一乃至第三の情報処理装置１１１，１１２，１１３の各装置においてプログラムが実行されることにより実現される各種の機能について説明する。図３は第一乃至第三の情報処理装置１１１，１１２，１１３の各装置において実現される各種の機能を示している。第二の情報処理装置１１２の対策済み脅威データ記憶部３０１は、第二のサイト１０２において策定され運用されている情報セキュリティポリシーに対応する内容を示す情報が記述されたデータである対策済み脅威データを記憶する機能である。対策済み脅威データは、対策済み脅威データ管理テーブルに管理されている。図４に対策済み脅威データ管理テーブルの一例を示している。対策済み脅威データは、脅威のカテゴリ別に分類されて管理されている。この図に示す対策済み脅威データ管理テーブル４００において、脅威カテゴリコード４０１の欄には、脅威カテゴリごとに固有に付与される識別子である脅威カテゴリコードが設定される。脅威カテゴリ４０２の欄には、脅威カテゴリの内容を示す文字列が設定される。対策済み脅威の欄４０３には、対策済み脅威データを特定する識別子が設定される。対策済み脅威リスト４０４の欄には対策済み脅威データの内容を示す文字列が設定される。

【００２１】

第二の情報処理装置１１２の対策済み脅威データ送信部３０２は、対策済み脅威データ記憶部３０１によって記憶されている対策済み脅威データ管理テーブル４００を、通信ネットワーク５０を介して第一の情報処理装置１１１に送信する機能である。対策済み脅威データ送信部３０２は、入力装置２０５からオペレータ等による操作入力を受け付け、これにより受け付けた入力に応じて第二の情報処理装置１１２が第一の情報処理装置１１１に対策済み脅威データ管理テーブル４００を送信するタイミングをスケジュールする機能を有する。対策済み脅威データ送信部３０２は、スケジュールしたタイミングが到来すると、対策済み脅威データ管理テーブル４００を自動的に第一の情報処理装置１１１に送信する機能を有する。なお、このときの送信タイミングとしては、例えば、即時実行、毎日、毎週、毎月、指定された日時等を設定することが可能である。

【００２２】

第三の情報処理装置１１３の脅威データ記憶部３０３は、通信ネットワーク５０において、もしくは、通信ネットワーク５０に接続している装置において、過去に生じた脅威に関する情報が記述されたデータである脅威データを記憶する機能を有する。第三の情報処理装置１１３は、例えば、脅威データ記憶部３０３が記憶している脅威データを更新する脅威データ更新部３０４を有する。脅威データ更新部３０４は、例えば、通信ネットワーク５０を介して当該通信ネットワーク５０に接続している装置から受信した脅威に関する情報に基づいて脅威データを更新する。また、脅威データ更新部３０４は、例えば、通信ネットワーク５０において生じた脅威を検知して、検知した脅威に対応する脅威データを

生成して記憶する。さらに、脅威データ更新部３０４は、入力装置２０５からのオペレータ等の入力操作や記録媒体２０７からのデータの読み出し等により脅威に関する情報の入力を受け付けて、受け付けた脅威に関する情報に対応する脅威データを生成し記憶する。

【００２３】

脅威データは、脅威データ管理テーブルに管理されている。図５に脅威データ記憶部３０３が記憶している脅威データ管理テーブルの一例を示している。本実施例において、脅威データは、脅威のカテゴリ別に分類されて管理されている。この図に示す脅威データ管理テーブル５００において、脅威カテゴリコードの欄５０１には、脅威カテゴリごとに固有に付与される識別子が設定される。脅威カテゴリと識別子との対応は、上述した対策済み脅威データ管理テーブル４００の場合と同様である。脅威カテゴリの欄５０２には、脅威カテゴリの内容を示す文字列が設定される。脅威コードの欄５０３には、脅威データを特定する識別子が設定される。脅威情報の欄５０４には、脅威データの内容を示す文字列が設定される。被害額の欄５０５には、その脅威により被害を受けた場合に生じる損害の大きさを示すデータである損害量データが設定される。損害量データとしては、例えば、脅威により第二のサイト１０２が被害を受けた場合に生じる被害額が採用される。

【００２４】

図５に例示している被害額は、上記あるサイトが一年間に受けると予想される被害総額である。この被害総額は、例えば、あるサイトが有効な情報セキュリティポリシーを運用していなかったために受けた脅威により生じた被害額と、そのサイトにおける過去一年間における脅威の発生確率とを用いて求められる。各脅威についての損害量データは、基本的に第３のサイト１０３において管理され、第三サイト１０３の運営者から第一のサイト１０１の運営者に適宜通知される。損害量データは、第三の情報処理装置１０３では管理せずに第一のサイト１０１において管理するような運用形態を採用することもできる。

【００２５】

第三の情報処理装置１１３の脅威データ送信部３０５は、脅威データ記憶部３０３が記憶している脅威データ管理テーブル５００の内容を通信ネットワーク５０を介して第一の情報処理装置１１１に送信する。脅威データ送信部３０５は、入力装置２０５からオペレータ等による操作入力を受け付けて、受け付けた入力に応じて第二の情報処理装置１１２が第一の情報処理装置１１１に脅威データ管理テーブル４００を送信するタイミングをスケジュールする。脅威データ送信部３０５は、スケジュールしたタイミングが到来すると、脅威データを第一の情報処理装置１１１に自動的に送信する機能を有する。このときの送信タイミングとしては、例えば、即時実行、毎日、毎週、毎月、指定された日時等を設定することが可能である。脅威データ送信部３０５は、脅威データ更新部３０４により脅威データ管理テーブル５００の内容が更新された場合に、脅威データ管理テーブル５００や更新差分を自動的に第一の情報処理装置１１１に送信するようにスケジュールする機能も有する。

【００２６】

第一の情報処理装置１１１の対応データ記憶部３１０は、脅威データと、脅威データが示す脅威に対して有効な情報セキュリティポリシーを示す対策済み脅威データとの対応を示すデータ（以後、対応データと称する）が記述された対応データ管理テーブルを記憶する機能である。図６に対応データ管理テーブル６００の一例を示している。対応データ管理テーブル６００には、脅威データと、その脅威データに対して有効な情報セキュリティポリシーである対策済み脅威との対応が記述されている。対策済み脅威コードの欄６０１には、対策済み脅威データを特定する識別子が設定される。対策済み脅威リスト６０２の欄には対策済み脅威データの内容を示す文字列が設定される。脅威コードの欄６０３には、対策済み脅威データに対応する脅威データを特定する識別子が設定される。脅威情報の欄６０４には、対策済み脅威データに対応する脅威データの内容を示す文字列が設定される。

【００２７】

第一の情報処理装置１１１の対策済み脅威データ受信部３１１は、第二の情報処理装置

１１２の対策済み脅威データ送信部３０２から送信されてくる対策済み脅威データ管理テーブル４００を受信して記憶する。第一の情報処理装置１１１の脅威データ受信部３１２は、第三の情報処理装置１１３の脅威データ送信部３０５から送信されてくる脅威データ管理テーブル５００を受信して記憶する。

【００２８】

第一の情報処理装置１１１の有効な対策済み脅威データ抽出部３１３は、前記対応データに基づいて、対策済み脅威データ受信部３１１が受信した前記対策済み脅威データの中から、前記脅威データ受信部３１２が受信した脅威データに、対応する脅威データが存在するものを抽出する。例えば、対策済み脅威データ受信部が図４の対策済み脅威データ管理テーブル４００を、また、脅威データ受信部５００が図５に示す脅威データ管理テーブル５００を受信したとする。この場合、当該対策済み脅威データ管理テーブル４００の対策済み脅威データ（対策済み脅威）のうち「Ｗｅｂサーバへの大量のアクセス」という対策済み脅威データは、図５の脅威データ管理テーブル５００に対応する脅威データが存在するので、当該対策済み脅威データは有効な対策済み脅威データ抽出部３１３による抽出の対象となる。

【００２９】

第一の情報処理装置１１１の評価データ生成部３１４は、有効な対策済み脅威データ抽出部３１３により抽出された前記対策済み脅威データを記載した評価データを生成する。ここで評価データ生成部３１４は、評価データの生成に際し、有効な対策済み脅威データ抽出部３１３により抽出された対策済み脅威データを、上述の対応データに対応づけられている脅威データについての損害量データの降順に整列する。第一の情報処理装置１１１の評価レポート出力部３１５は、評価データ生成部３１４により生成された評価データを記載した評価レポートを第一の情報処理装置１１１のディスプレイやプリンタ等の出力装置２０６に出力する。第一の情報処理装置１１１の評価レポート送信部３１６は、電子メール等により通信ネットワーク５０を介して評価レポートを第二の情報処理装置１１２に送信する。

【００３０】

図７に評価レポートの一例を示している。この図に示す評価レポート７００の、効果の順位の欄７０１には、損害量データの降順に整列された対策済み脅威データの順位が記載される。対策済み脅威の欄７０２には、対策済み脅威データに対応する情報セキュリティポリシーの内容が記載される。未対策時の被害額の欄７０３には、損害量データが記載される。この図において、未対策時の被害額の欄７０３に記載される損害量データは想定した被害額としている。

【００３１】

ここで評価レポート７００に記載されている対策済み脅威データが示す情報セキュリティポリシーは、実際に生じた脅威に対して有効であった情報セキュリティポリシーである。従って、評価レポートに基づいて、第二のサイト１０２において策定され運用されている情報セキュリティポリシーの妥当性を評価することができる。このように第一のサイト１０１において第二のサイト１０２における情報セキュリティポリシーの妥当性を示す評価レポートが作成されることで、顧客である第二のサイト１０２を運営する企業等の組織は、自らが策定し運用を行っている情報セキュリティポリシーの評価や見直しのために、自ら脅威に関する情報の収集を行う手間が軽減される。また、第二のサイト１０２を運営する組織は、情報セキュリティポリシーの評価や見直しを行うために必要とされる技術水準を維持するための管理負担からも開放される。従って、第二のサイト１０２を運営する組織では、情報セキュリティポリシーの評価や見直しを効率よく行うことができる。また、第三の情報処理装置１１３から送信されてくる、過去に生じた脅威を示すデータである脅威データに基づいて情報セキュリティポリシーの評価や見直しが行われることになるため、評価が客観的に行われて、第二のサイト１０２において策定され運用されている情報セキュリティポリシーについて、その効果や有効性についての適切な評価や見直しを行うことが可能となる。また本実施例の評価レポートは単に未対策の脅威を指摘したレポート

とは異なり、既に運用されている情報セキュリティポリシーの効果、価値、有効性等についての評価を記載したものである。従って、評価レポートは、経営層（社長、情報セキュリティ担当役員などの上位経営管理者等）や組織のメンバー（従業員等）に情報セキュリティポリシーの効果、価値、有効性等を理解させ遵守させる動機付けとなる有用な資料となり、評価レポートを活用することで組織における情報セキュリティマネージメントの円滑的な運用が促進されることとなる。さらに、評価レポートにおいて、対策済み脅威データは損害量データの降順に整列されている。ここで上述したように損害量データは例えば脅威により第二のサイト１０２が被害を受けた場合に生じる被害額である。このように対策済み脅威データが損害量データの降順に整列されていることで、例えば、顧客は評価レポートを参照することにより、効果の高かった情報セキュリティポリシーがいずれであるのかを容易に把握することができる。

【００３２】

第一の情報処理装置１１１の未対策脅威データ抽出部３１７は、前記対応データに基づいて、脅威データ受信部３１２が受信した前記脅威データの中から、対応する対策済み脅威データが、対策済み脅威データ受信部３１１が受信した前記対策済み脅威データ中に存在しない脅威データを抽出する。例えば、図５の脅威データ管理テーブル５００の脅威データのうち「大量のＩＣＭＰパケットの受信」という脅威データは、対応する対策済み脅威データが図４の対策済み脅威データ管理テーブル４００中に存在しないので、当該脅威データは未対策脅威データ抽出部３１７による抽出対象となる。

【００３３】

第一の情報処理装置１１１の評価データ生成部３１４は、未対策脅威データ抽出部３１７により抽出された前記脅威データを記載した評価データを生成する。ここで評価データ生成部３１４は、評価データの生成に際し、未対策脅威データ抽出部３１７により抽出された脅威データを上述の対応データに対応づけられている脅威データについての損害量データの降順に整列する。第一の情報処理装置１１１の評価レポート出力部３１５は、評価データ生成部３１４により生成された評価データを記載した評価レポートを第一の情報処理装置１１１のディスプレイやプリンタ等の出力装置２０６に出力する。第一の情報処理装置１１１の評価レポート送信部３１６は、評価レポートを電子メール等により通信ネットワーク５０を介して第二の情報処理装置１１２に送信する。

【００３４】

図８に評価レポートの一例を示している。この図に示す評価レポート８００の改訂優先順位の欄８０１には、損害量データの降順に整列された脅威データの優先順位が記載される。優先順位が高いほど、情報セキュリティポリシーを優先的に策定する必要性の高い脅威であるといえる。未対策脅威の欄８０２には、脅威データに対応する脅威の内容が記載される。想定被害額の欄８０３には、損害量データが記載される。

【００３５】

ここでこの評価レポート８００に記載されている脅威データが示す脅威は、実際に生じた脅威であって、その脅威に対し第二のサイト１０２では何ら有効な情報セキュリティポリシーの運用がなされていなかった脅威である。従って、この評価レポートは、例えば、第二のサイト１０２では、次回の情報セキュリティポリシーの改訂時に優先的に対策を講ずるべき脅威を示した情報として利用される。このように第二のサイト１０２において不足している情報セキュリティポリシーを示した評価レポートが第一のサイト１０１において自動的に作成されることで、第二のサイト１０２を運営する企業等の組織は、自らが策定し運用を行っている情報セキュリティポリシーの評価や見直しのために、自ら脅威に関する情報の収集を行う手間が軽減される。また、第二のサイト１０２を運営する組織は、情報セキュリティポリシーの評価や見直しを行うために必要とされる技術水準を維持するための管理負担からも開放される。従って、第二のサイト１０２を運営する組織では、情報セキュリティポリシーの評価や見直しを効率よく行うことができる。また第三の情報処理装置１１３から送信されてくる過去に生じた脅威を示すデータである脅威データに基づいて情報セキュリティポリシーの評価や見直しが行われることになるため、評価は客観的

に行われることとなり、第二のサイト１０２において策定され運用されている情報セキュリティポリシーについて、その効果、価値、有効性等についての適切な評価や見直しを行うことが可能となる。また本実施例の評価レポートは単に未対策の脅威を指摘したレポートとは異なり、既に運用されている情報セキュリティポリシーの効果、価値、有効性等についての評価を記載したものである。従って、評価レポートは、経営層（社長、情報セキュリティ担当役員などの上位経営管理者等）や組織のメンバー（従業員等）に情報セキュリティポリシーの効果、価値、有効性等を理解させ遵守させる動機付けとなる有用な資料となり、評価レポートを活用することで組織における情報セキュリティマネージメントの円滑的な運用が促進されることとなる。さらに、評価レポートにおいて、脅威データは損害量データの降順に整列されている。ここで上述したように損害量データは例えば脅威により第二のサイト１０２が被害を受けた場合に生じる被害額である。このように脅威データが損害量データの降順に整列されていることで、例えば顧客は評価レポートを参照することにより、情報セキュリティポリシーの改訂時等において、優先的に考慮すべき脅威を容易に把握することができる。

【００３６】

次に、本実施例の情報セキュリティポリシー評価システムにより、第二のサイト１０２において策定され運用されている情報セキュリティポリシーについての評価に関する処理の流れを、図９に示すフローチャートとともに説明する。

【００３７】

まず、第二の情報処理装置１１２の対策済み脅威データ送信部３０２は、対策済み脅威データ記憶部３０１が記憶している対策済み脅威データ管理テーブル４００を所定のタイミングで第一の情報処理装置１１１に送信する（S911）。第一の情報処理装置１１１の対策済み脅威データ受信部３１１は、送信されてくる対策済み脅威データ管理テーブル４００を受信して記憶する（S912）。

第三の情報処理装置１１３の脅威データ送信部３０５は、脅威データ記憶部３０３が記憶している脅威データ管理テーブル５００を所定のタイミングで第一の情報処理装置１１１に送信する（S913）。第一の情報処理装置１１１の脅威データ受信部３１２は、脅威データ管理テーブル５００を受信して記憶する（S914）。

【００３８】

次に、第一の情報処理装置１１１の有効な対策済み脅威データ抽出部３１３は、前記対応データに基づいて、対策済み脅威データ受信部３１１が受信した前記対策済み脅威データの中から、前記脅威データ受信部３１２が受信した脅威データに、対応する脅威データが存在するものを抽出する（S915）。また、第一の情報処理装置１１１の未対策脅威データ抽出部３１７は、前記対応データに基づいて、脅威データ受信部３１２が受信した前記脅威データの中から、対応する対策済み脅威データが、対策済み脅威データ受信部３１１が受信した前記対策済み脅威データ中に存在しない脅威データを抽出する（S916）。

【００３９】

次に、評価データ生成部３１４は、抽出された対策済み脅威データを記載した評価データを生成する（S917）。評価レポート出力部３１５は、評価データ生成部３１４により生成された評価データを記載した評価レポートを第一の情報処理装置１１１のディスプレイやプリンタ等の出力装置２０６に出力する（S918）。第一の情報処理装置１１１の評価レポート送信部３１６は、電子メール等により通信ネットワークを介して第二の情報処理装置１１２に評価レポートを送信する（S919）。

【００４０】

ところで、以上に説明した実施例では、対策済み脅威データを第二の情報処理装置１１２において記憶しておき、これを第一の情報処理装置１１１に送信するようにしているが、顧客のサイトである第二のサイトにおいて対策済み脅威データを管理する管理負担を無くすため、例えば、次のような形態とすることも考えられる。すなわち、まず、第二の情報処理装置１１２において、第二のサイトで運用されている情報セキュリティポリシーを示すデータであるポリシーデータを記憶しておく（ポリシーデータ記憶部）。第二の情報

処理装置は、ポリシーデータを第一の情報処理装置１１１に送信する（ポリシーデータ送信部）。第一の情報処理装置１１１は、前記ポリシーデータを受信する（ポリシーデータ受信部）。第一の情報処理装置１１１は、脅威データと、脅威データが示す脅威に対して有効な情報セキュリティポリシーを示すポリシーデータとの対応を示すデータである対応データを記憶しておく。そして、第一の情報処理装置１１１は、前記対応データに基づいて、受信した前記ポリシーデータの中から、脅威データ受信部３１２が受信した脅威データに、対応する脅威データが存在するポリシーデータを抽出し（有効なポリシーデータ抽出部）、抽出した前記ポリシーデータを記載した評価データを生成するようにする。また第一の情報処理装置１１１は、前記対応データに基づいて、脅威データ受信部３１２が受信した脅威データの中から、前記ポリシーデータ受信部が受信した前記ポリシーデータ中に、対応するポリシーデータが存在しない脅威データを抽出し、抽出した脅威データを記載した評価データを生成するようにする。このような構成とすることで、第二の情報処理装置１１２では、第二のサイトで運用されている情報セキュリティポリシーを示すデータであるポリシーデータを管理してさえいればよく、対策済み脅威データを管理する必要が無くなる。

【００４１】

＝＝＝第二実施例＝＝＝

図１０は本発明の第二実施例として説明する情報セキュリティポリシー評価システム（ポリシー評価システム）の概略構成を示している。この図において、第一のサイト１０１は、例えば、顧客からの依頼に応じて第二のサイト１０２で運用されている情報セキュリティポリシーの評価を行う評価業者のサイトである。例えば、システムコンサルタント業務やシステム監査業務を営む組織が上記評価業者となりうる。第二のサイト１０２は、例えば、情報セキュリティポリシーの評価を依頼する顧客のサイトである。第三のサイト１０３は、例えば、脅威に関する情報を収集しその提供を行っている脅威情報を提供する脅威情報提供業者のサイトである。例えば、インターネットの接続サービスを行っているインターネットサービスプロバイダは、ＤｏＳやＤＤｏＳ等の不正アクセスに関する情報を把握していることが多いので、これらのものは上記脅威情報提供業者となりうる。第四のサイト１０４は第二のサイト１０２を運営する顧客を加入者とし、第二のサイト１０２が脅威を受けた場合に生じる損害を補償する保険を商品とする保険業を運営する保険業者のサイトである。第四のサイト１０４には第四の情報処理装置１１４が設けられている。

【００４２】

第一乃至第四の情報処理装置１１１，１１２，１１３，１１４のハードウエア構成は、第一実施例と同様であるのでここでは説明を省略する。図１１は本発明の第二実施例にかかる第一乃至第四の情報処理装置１１１，１１２，１１３，１１４の各装置において実現される各種の機能を示す図である。この図に示すように、第一乃至第三の情報処理装置１１１，１１２，１１３では、各装置においてプログラムが実行されることにより第一実施例と同様の機能が実現されている。なお、第一実施例の構成に加え、第一の情報処理装置１１１の評価レポート送信部３１６は、通信ネットワーク５０を介して第四の情報処理装置１１４に送信する機能を有する。第四の情報処理装置１１４は、第一の情報処理装置１１１から送信されてくる前記評価レポートを受信する評価レポート受信部３２０を有する。さらに、第四の情報処理装置１１４は、記憶している前記補償額を、前記評価データ受信部により受信した前記評価レポートに応じて決定される前記補償額に設定する補償額設定部３２１を有する。

【００４３】

図１２は以上の構成からなるポリシー評価システムを用いて実施されるビジネスの一形態を説明している。このビジネス形態では、第二のサイト１０２の顧客が、第三のサイト１０３の評価業者に情報セキュリティポリシーの評価を依頼するための登録を行うとともに情報セキュリティポリシーの評価を依頼するための評価手数料を支払う。ここで評価の依頼登録や評価手数料の支払いは、例えば、評価業者が提供する登録用のWebページにアクセスすることにより行うことができる。評価業者は、登録された依頼を受諾するととも

に顧客から前記評価手数料を受け取る（S1201）。

【００４４】

評価業者は、受け取った評価手数料の一部を情報提供料として脅威情報提供業者に支払う（S1202）。評価業者は、受け取った前記評価手数料の一部を顧客が上記保険のために支払う保険料として保険業者に支払う（S1203）。

顧客は評価業者に対し、顧客が第二のサイト１０２において策定し運用を行っている情報セキュリティポリシー（対策済み脅威リスト）を提供する（S1204）。これは具体的には第一実施例で説明したように、第二の情報処理装置１１２から第一の情報処理装置１１１に対策済み脅威データ管理テーブル４００が送信されることにより行われる。

脅威情報提供業者は、評価業者に対し、過去に生じた脅威に関する情報を提供する（S1205）。これは具体的には第一実施例で説明したように、第三の情報処理装置１１３から第一の情報処理装置１１１に脅威データ管理テーブル５００が送信されることにより行われる。

【００４５】

評価業者は、顧客から入手した情報セキュリティポリシーと、脅威情報提供業者から入手した脅威に関する情報とをマッチングすることにより、評価レポートを作成する（S1206）。これらの処理は、第一実施例において説明したように、有効な対策済み脅威データ抽出部３１３、未対策脅威データ抽出部３１７、及び、評価データ生成部３１４の処理により行われる。

評価業者は、評価レポートを顧客及び保険業者に送付する（S1207）。この送付は、第一の情報処理装置１１１から第一及び第四の情報処理装置１１４に評価レポートをデータ伝送や電子メール等により送信すること等により行われる。第四の情報処理装置１１４では、評価レポートは評価レポート受信部３２０により受信される。

【００４６】

保険業者は、顧客が前記情報セキュリティポリシーに従って適切に運用を行っているかどうかを監査して（S1208）、その結果を記載した監査レポートを作成する（S1209）。保険業者は、評価レポートと監査レポートを参酌して補償額を決定する。保険業者は、例えば、評価レポートや監査レポートの内容から、第二のサイト１０２の顧客が策定し運用を行っている情報セキュリティポリシーの効果や価値、有効性が高いと判断した場合には、保険料を同額に保ったまま保険の補償額を増額する。逆に評価レポートや監査レポートの内容から、第二のサイト１０２の顧客が策定し運用を行っている情報セキュリティポリシーの効果や価値、有効性が低いと判断される場合には、保険料を同額に保ったまま保険の補償額を減額する。第四の情報処理装置１１４の補償額設定部３２１は、保険の補償額を記憶しており、上記決定により補償額が変更されると記憶している補償額を変更された補償額に設定し直す（S1210）。

【００４７】

このように第二実施例のポリシー評価システムによれば、第二のサイト１０２の顧客は、同じ保険料で保険の補償額を増額するためもしくは減額されないように、適切な情報セキュリティポリシーを策定するよう努力するようになる。一方、保険業者は、不適切な情報セキュリティポリシーを運用している顧客に対し高い補償額を設定してしまうというリスクを回避することができる。また適切な情報セキュリティポリシーを策定し運用を行っている顧客はより適切な補償額を設定してもらえるという付加価値のある保険を選定するようになる。このため、保険の加入者が増えて保険業者の収益増大に繋がることとなる。また保険の加入者が増える結果、評価業者の顧客も増えて評価業者の収益も増大し、さらに脅威情報提供業者の収益も増大する。このように本実施例のポリシー評価システムによれば、顧客、評価業者、脅威情報提供者、保険業者の全ての者が何らかのメリットを享受できることになる。

【００４８】

＝＝＝第三実施例＝＝＝

図１３は本発明の第三実施例として説明する情報セキュリティポリシー評価システム（

ポリシー評価システム）の概略構成を示している。この実施例では、第二実施例において第四のサイト１０４の機能を第一のサイト１０１に持たせるようにしたものである。第一のサイト１０１を運営する上記評価業者は同時に保険業者でもあり、第四の情報処理装置１１４は、第一の情報処理装置１１１を運営する組織と同じ組織によって運営されている。

【００４９】

図１４はこのような形態からなるポリシー評価システムを用いて行われるビジネスの一例を説明している。第二のサイト１０２の顧客は、第三のサイト１０３の評価業者（保険業者でもある）に情報セキュリティポリシーの評価を依頼するための登録を行うとともに情報セキュリティポリシーの評価を依頼するための評価手数料を支払う。ここで評価の依頼登録や評価手数料の支払いは、例えば評価業者が提供する登録用のWebページにアクセスすることにより行うことができる。評価業者は登録された依頼を受諾するとともに顧客から前記評価手数料を受け取る（S1401）。

【００５０】

評価業者は、受け取った評価手数料の一部を情報提供料として脅威情報提供業者に支払う（S1402）。なお、評価業者（保険業者でもある）は、受け取った前記評価手数料の一部を顧客が上記保険のために支払う保険料として充当する。

顧客は評価業者に対し、顧客が第二のサイト１０２において策定し運用を行っている情報セキュリティポリシー（対策済み脅威リスト）を提供する（S1404）。これは第一実施例で説明したように、第二の情報処理装置１１２から第一の情報処理装置１１１に対策済み脅威データ管理テーブル４００が送信されることにより行われる。

脅威情報提供業者は、評価業者に対し、過去に生じた脅威に関する情報を提供する（S1405）。これは第一実施例で説明したように、第三の情報処理装置１１３から第一の情報処理装置１１１に脅威データ管理テーブル５００が送信されることにより行われる。

【００５１】

評価業者は、顧客から入手した情報セキュリティポリシーと、脅威情報提供業者から入手した脅威に関する情報とをマッチングすることにより、評価レポートを作成する（S1406）。これらの処理は、第一実施例で説明したように、有効な対策済み脅威データ抽出部３１３、未対策脅威データ抽出部３１７、及び、評価データ生成部３１４の機能により行われる。

評価業者は、評価レポートを顧客に送付する（S1407）。この送付は、例えば、第一の情報処理装置から第二の情報処理装置１１２に評価レポートをデータ伝送や電子メール等により送信することにより行われる。

【００５２】

評価業者（保険業者でもある）は、顧客が前記情報セキュリティポリシーに従って適切に運用を行っているかどうかを監査し（S1408）、その結果を記載した監査レポートを作成する（S1409）。評価業者は、評価レポートと監査レポートとを参酌して補償額を決定する。評価業者は、例えば、評価レポートや監査レポートの内容から、第二のサイト１０２の顧客が策定し運用を行っている情報セキュリティポリシーの効果や価値、有効性が高いと判断した場合には、保険料を同額に保ったまま保険の補償額を増額する。逆に評価レポートや監査レポートの内容から、第二のサイト１０２の顧客が策定し運用を行っている情報セキュリティポリシーの効果や価値、有効性等が低いと判断される場合には、保険料を同額に保ったまま保険の補償額を減額する。第四の情報処理装置１１４の補償額設定部は保険の補償額を記憶しており、上記決定により補償額が変更されると記憶している補償額を変更された補償額に設定し直す（S1410）。

【００５３】

このように第三実施例のポリシー評価システムによれば、第二のサイト１０２の顧客は、同じ保険料で保険の補償額を増額するためもしくは減額されないよう、適切な情報セキュリティポリシーを策定するよう努力するようになる。一方、保険業者でもある評価業者は、不適切な情報セキュリティポリシーを運用している顧客に対し高い補償額を設定して

しまうというリスクを回避することができる。また適切な情報セキュリティポリシーを策定し運用を行っている顧客はより高額の補償額を設定してもらえる付加価値のある保険を選定するようになる。このため、保険加入者が増えて評価業者の収益増大に繋がることとなる。また保険の加入者が増える結果、評価業者の収益も増大し、脅威情報提供業者の収益も増大する。このように本実施例のポリシー評価システムによれば、顧客、保険業者でもある評価業者、脅威情報提供者の全ての者が何らかのメリットを享受できることになる。

【００５４】

以上の説明は本発明の理解を容易にするためのものであり、本発明を限定するものではない。本発明はその趣旨を逸脱することなく変更、改良され得ると共に本発明にはその等価物が含まれることは勿論である。

【図面の簡単な説明】

【００５５】

【図１】本発明の第一実施例にかかる情報セキュリティポリシー評価システムの概略構成を示す図である。

【図２】本発明の実施例にかかる第一乃至第三の情報処理装置のハードウエア構成を示す図である。

【図３】本発明の実施例にかかる第一乃至第三の情報処理装置の各装置において実現される各種の機能を示す図である。

【図４】本発明の実施例にかかる対策済み脅威データ管理テーブルの一例を示す図である。

【図５】本発明の実施例にかかる脅威データ管理テーブルの一例を示す図である。

【図６】本発明の実施例にかかる対応データ管理テーブルの一例を示す図である。

【図７】本発明の実施例にかかる評価レポート（対策して効果の高かった脅威）の一例を示す図である。

【図８】本発明の実施例にかかる評価レポート（ポリシー改訂時に考慮すべき脅威）の一例を示す図である。

【図９】本発明の実施例にかかる情報セキュリティポリシーについての評価に関する処理の流れを説明するフローチャートを示す図である。

【図１０】本発明の第二実施例にかかる情報セキュリティポリシー評価システムの概略構成を示す図である。

【図１１】本発明の第二実施例にかかる第一乃至第四の情報処理装置の各装置において実現される各種の機能を示す図である。

【図１２】本発明の第二実施例にかかるポリシー評価システムを用いて行われるビジネスの一形態を説明する図である。

【図１３】本発明の第三実施例にかかる第一乃至第四の情報処理装置の各装置において実現される各種の機能を示す図である。

【図１４】本発明の第三実施例にかかるポリシー評価システムを用いて行われるビジネスの一形態を説明する図である。

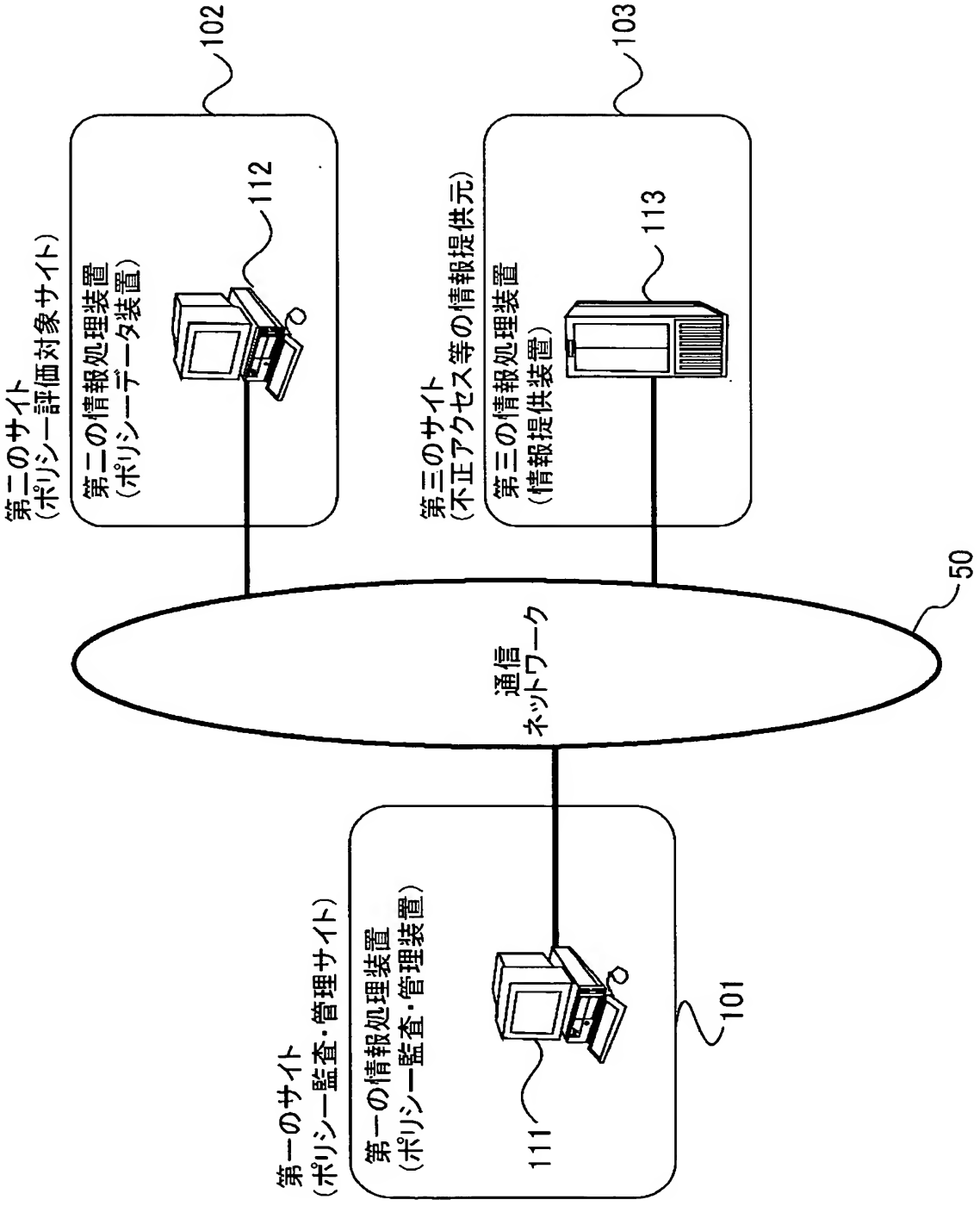
【符号の説明】

【００５６】

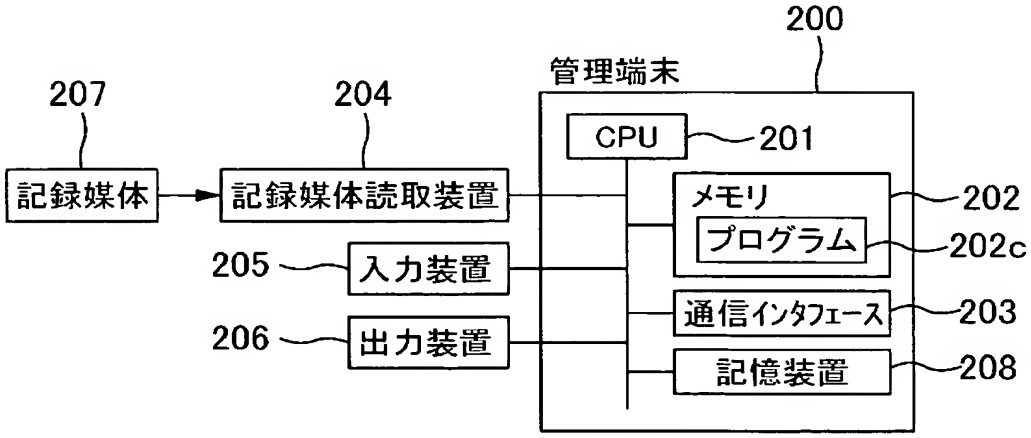
１０１　第一のサイト（評価業者のサイト）
１０２　第二のサイト（顧客のサイト）
１０３　第三のサイト（脅威情報提供業者のサイト）
１１１　第一の情報処理装置
１１２　第二の情報処理装置
１１３　第三の情報処理装置
３０１　対策済み脅威データ記憶部
３０２　対策済み脅威データ送信部
３０３　脅威データ記憶部

３０４　脅威データ更新部
３０５　脅威データ送信部
３１０　対応データ記憶部
３１１　対策済み脅威データ受信部
３１２　脅威データ受信部
３１３　有効な対策済み脅威データ抽出部
３１４　評価データ生成部
３１５　評価レポート出力部
３１６　評価レポート送信部
３１７　未対策脅威データ抽出部
３２０　評価レポート受信部
３２１　補償額設定部
４００　対策済み脅威データ管理テーブル
５００　脅威データ管理テーブル
６００　対応データ管理テーブル
７００　評価レポート（対策して効果の高かった脅威）
８００　評価レポート（ポリシー改訂時に考慮すべき脅威）

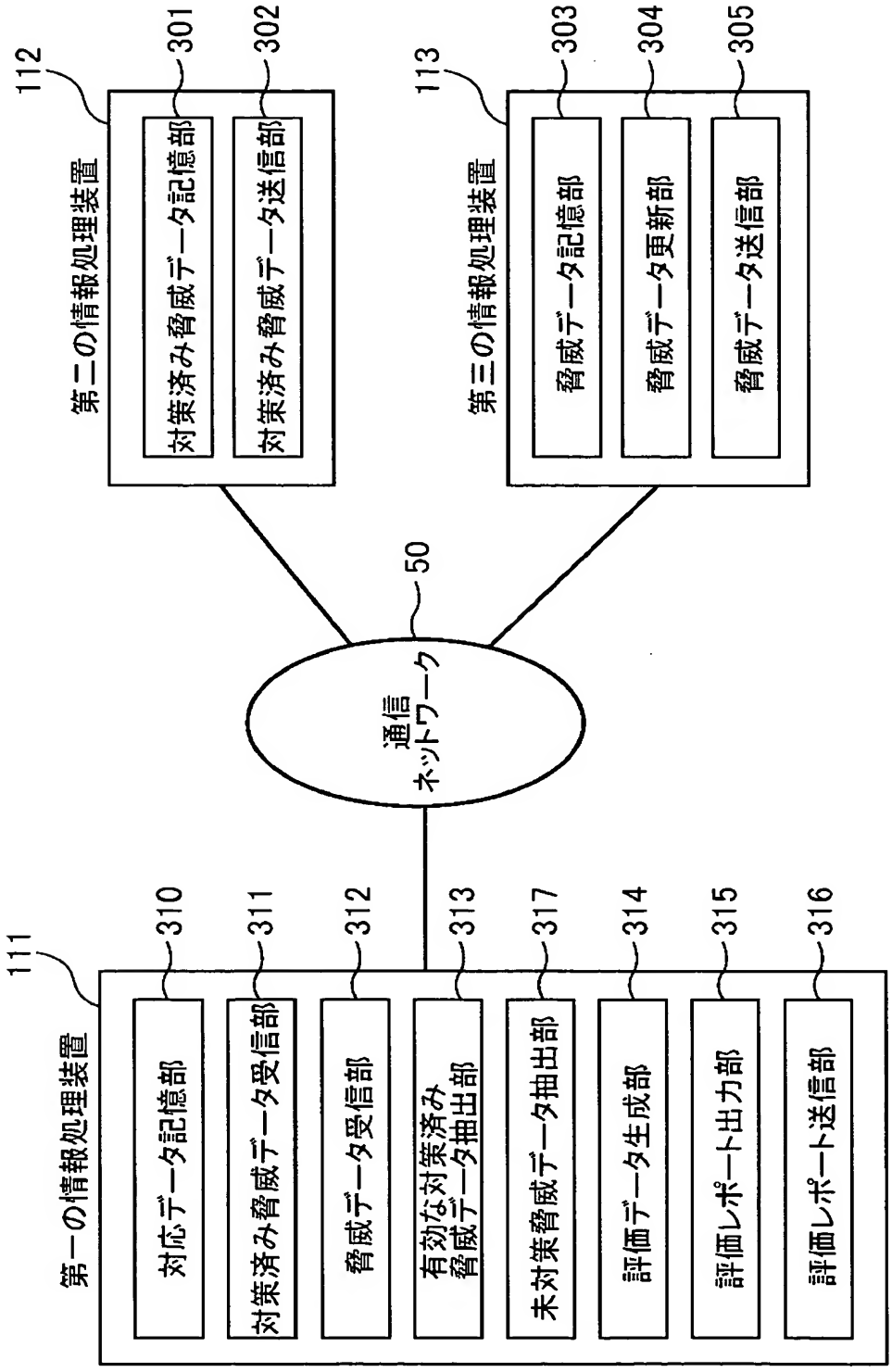
【書類名】図面
【図１】


第二のサイト
(ポリシー評価対象サイト)
第二の情報処理装置
(ポリシーデータ装置)
102
112
第三のサイト
(不正アクセス等の情報提供元)
第三の情報処理装置
(情報提供装置)
103
113
通信
ネットワーク
50
第一のサイト
(ポリシー監査・管理サイト)
第一の情報処理装置
(ポリシー監査・管理装置)
101
111

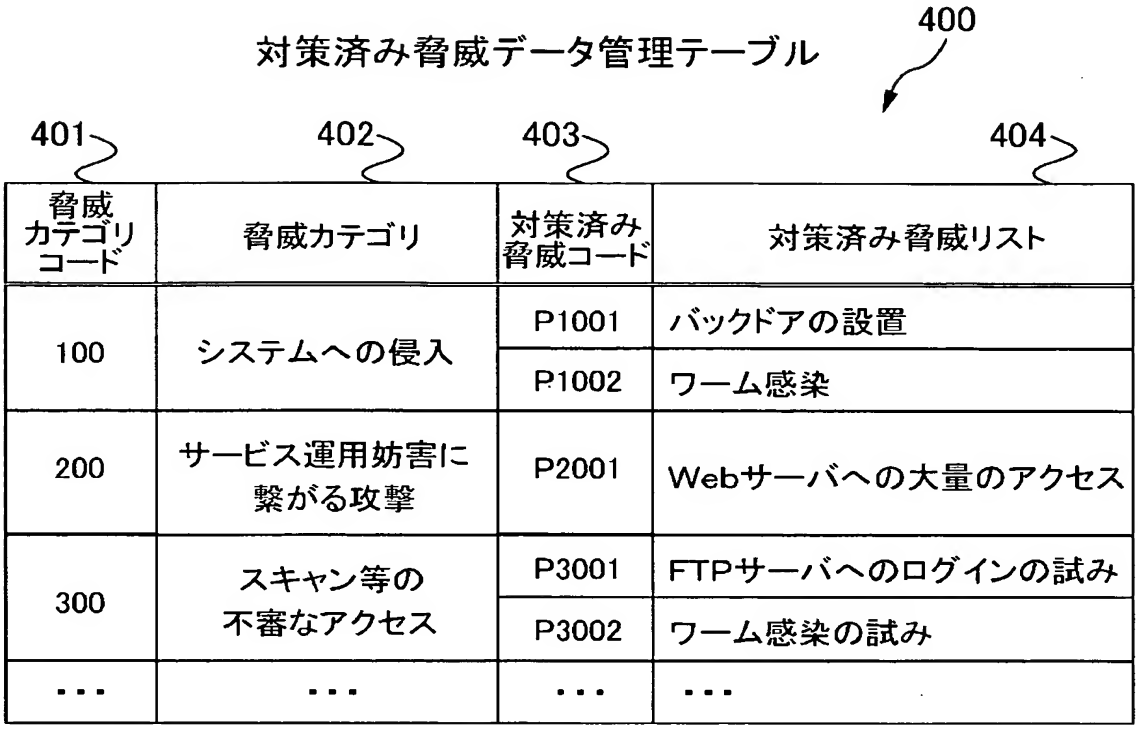
【図２】


200
管理端末
207
204
CPU
201
記録媒体
記録媒体読取装置
メモリ
202
プログラム
202c
205
入力装置
通信インタフェース
203
206
出力装置
記憶装置
208

【図３】

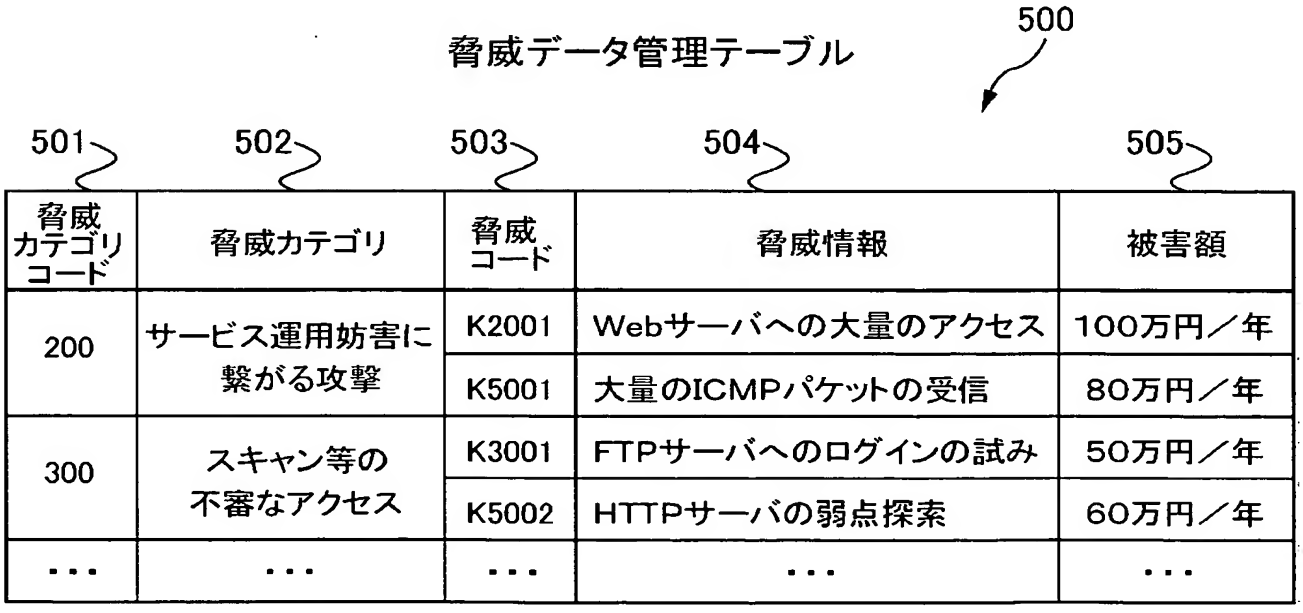

112
301
302
第二の情報処理装置
対策済み脅威データ記憶部
対策済み脅威データ送信部
113
303
304
305
第三の情報処理装置
脅威データ記憶部
脅威データ更新部
脅威データ送信部
50
通信
ネットワーク
111
310
311
312
313
317
314
315
316
第一の情報処理装置
対応データ記憶部
対策済み脅威データ受信部
脅威データ受信部
有効な対策済み
脅威データ抽出部
未対策脅威データ抽出部
評価データ生成部
評価レポート出力部
評価レポート送信部

【図４】



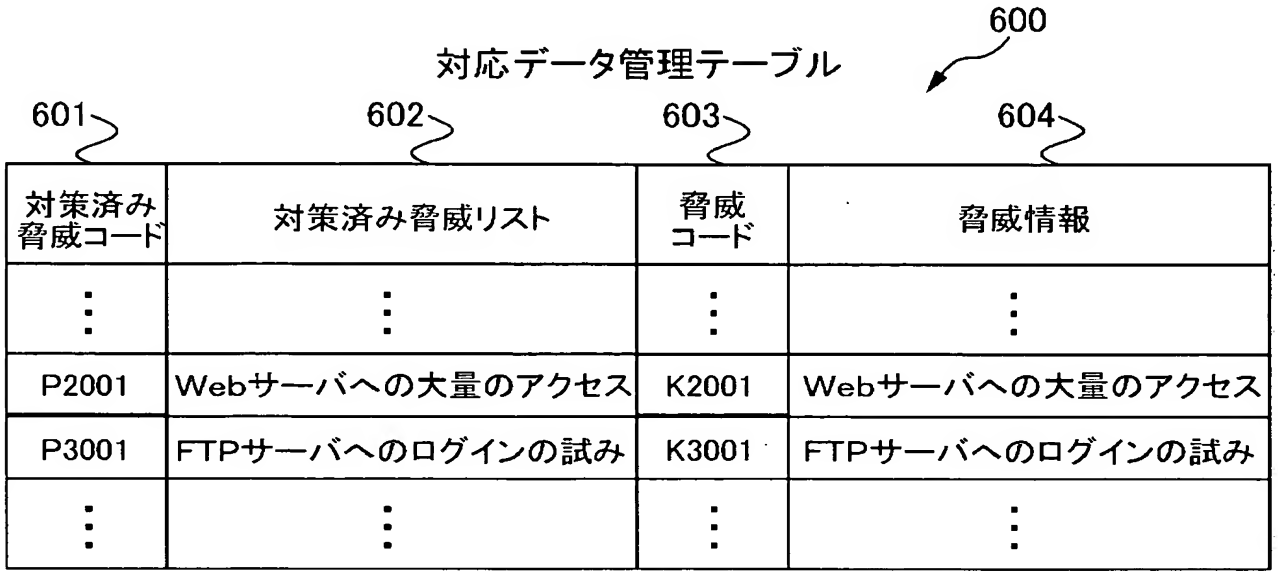

| 脅威カテゴリコード | 脅威カテゴリ | 対策済み脅威コード | 対策済み脅威リスト |
|---|---|---|---|
| 100 | システムへの侵入 | P1001 | バックドアの設置 |
| | | P1002 | ワーム感染 |
| 200 | サービス運用妨害に繋がる攻撃 | P2001 | Webサーバへの大量のアクセス |
| 300 | スキャン等の不審なアクセス | P3001 | FTPサーバへのログインの試み |
| | | P3002 | ワーム感染の試み |
| ・・・ | ・・・ | ・・・ | ・・・ |

【図５】



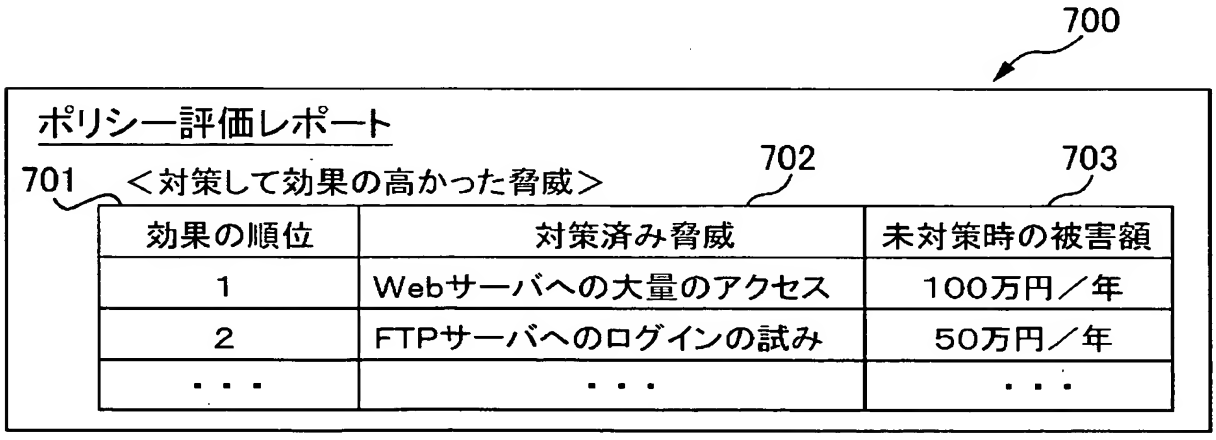

| 脅威カテゴリコード | 脅威カテゴリ | 脅威コード | 脅威情報 | 被害額 |
|---|---|---|---|---|
| 200 | サービス運用妨害に繋がる攻撃 | K2001 | Webサーバへの大量のアクセス | 100万円／年 |
| | | K5001 | 大量のICMPパケットの受信 | 80万円／年 |
| 300 | スキャン等の不審なアクセス | K3001 | FTPサーバへのログインの試み | 50万円／年 |
| | | K5002 | HTTPサーバの弱点探索 | 60万円／年 |
| ・・・ | ・・・ | ・・・ | ・・・ | ・・・ |

【図６】



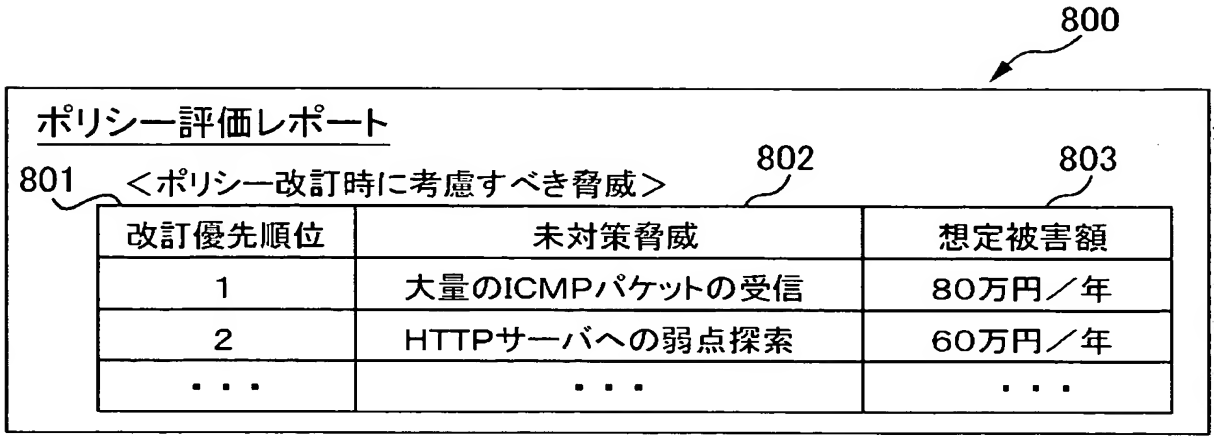

| 対策済み脅威コード | 対策済み脅威リスト | 脅威コード | 脅威情報 |
|---|---|---|---|
| ⋮ | ⋮ | ⋮ | ⋮ |
| P2001 | Webサーバへの大量のアクセス | K2001 | Webサーバへの大量のアクセス |
| P3001 | FTPサーバへのログインの試み | K3001 | FTPサーバへのログインの試み |
| ⋮ | ⋮ | ⋮ | ⋮ |

【図７】

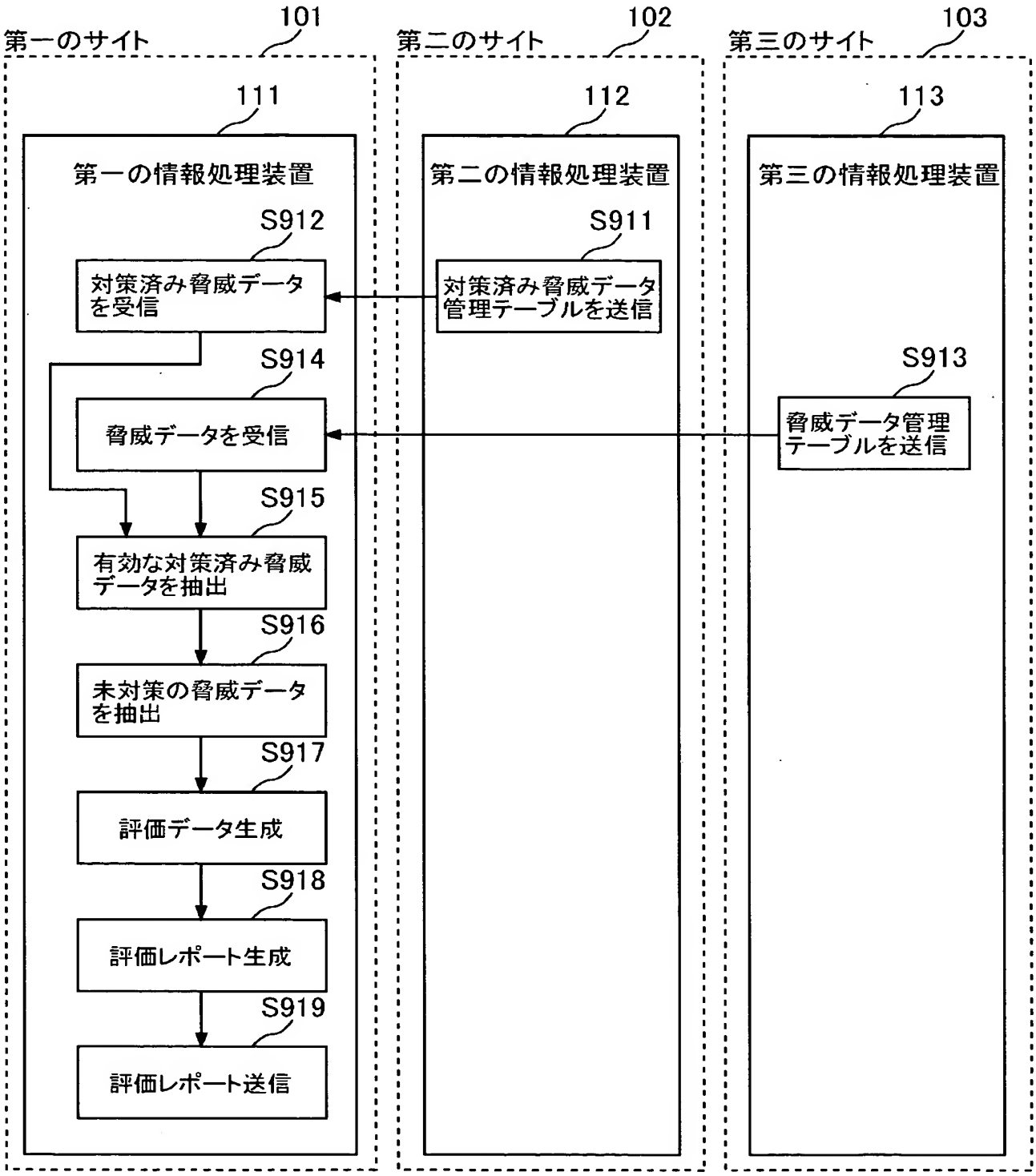



| 効果の順位 | 対策済み脅威 | 未対策時の被害額 |
|---|---|---|
| 1 | Webサーバへの大量のアクセス | 100万円／年 |
| 2 | FTPサーバへのログインの試み | 50万円／年 |
| ・・・ | ・・・ | ・・・ |

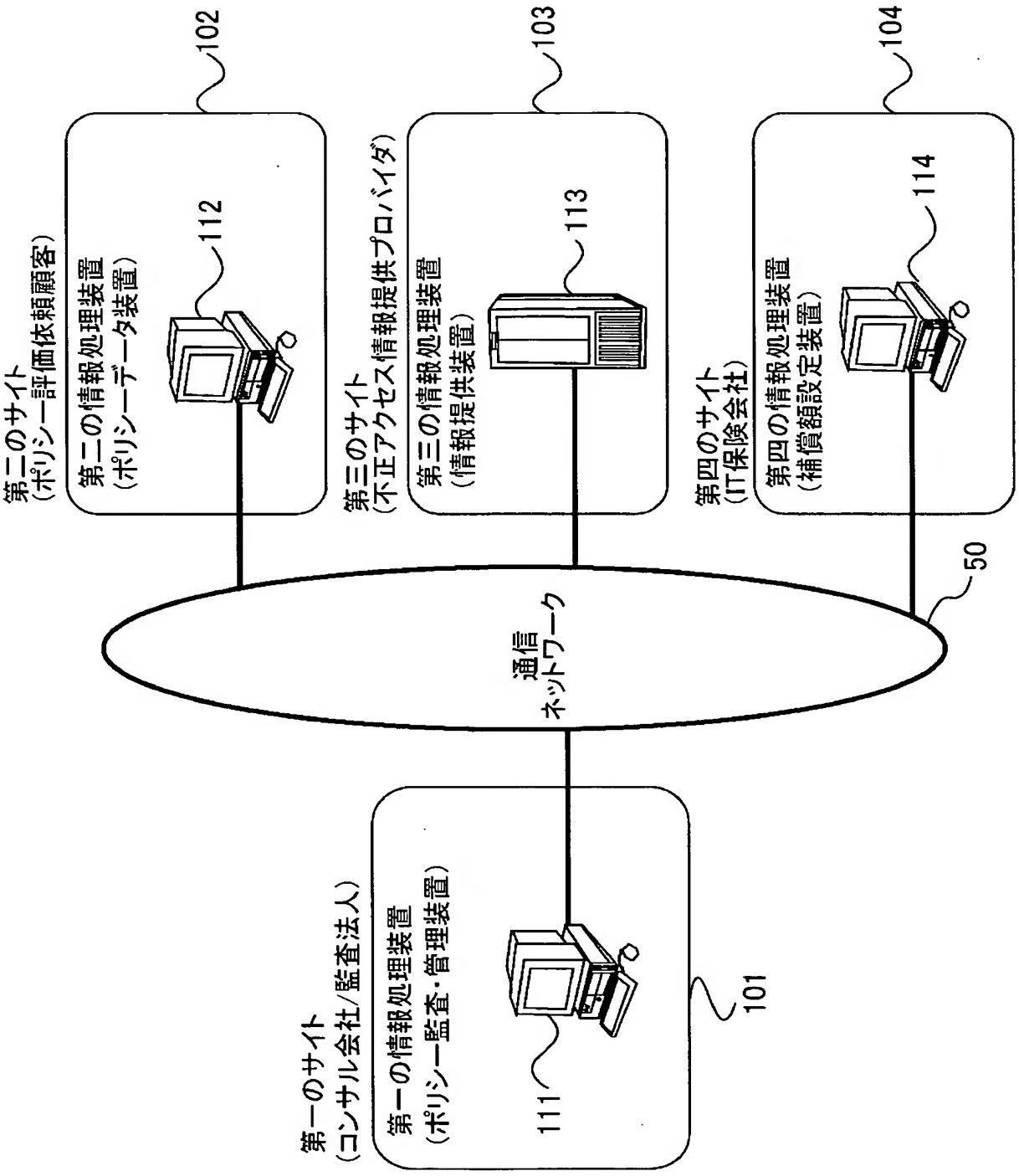
【図８】


800
ポリシー評価レポート
801
＜ポリシー改訂時に考慮すべき脅威＞
802
803
改訂優先順位
未対策脅威
想定被害額
1
大量のICMPパケットの受信
80万円／年
2
HTTPサーバへの弱点探索
60万円／年
・・・
・・・
・・・

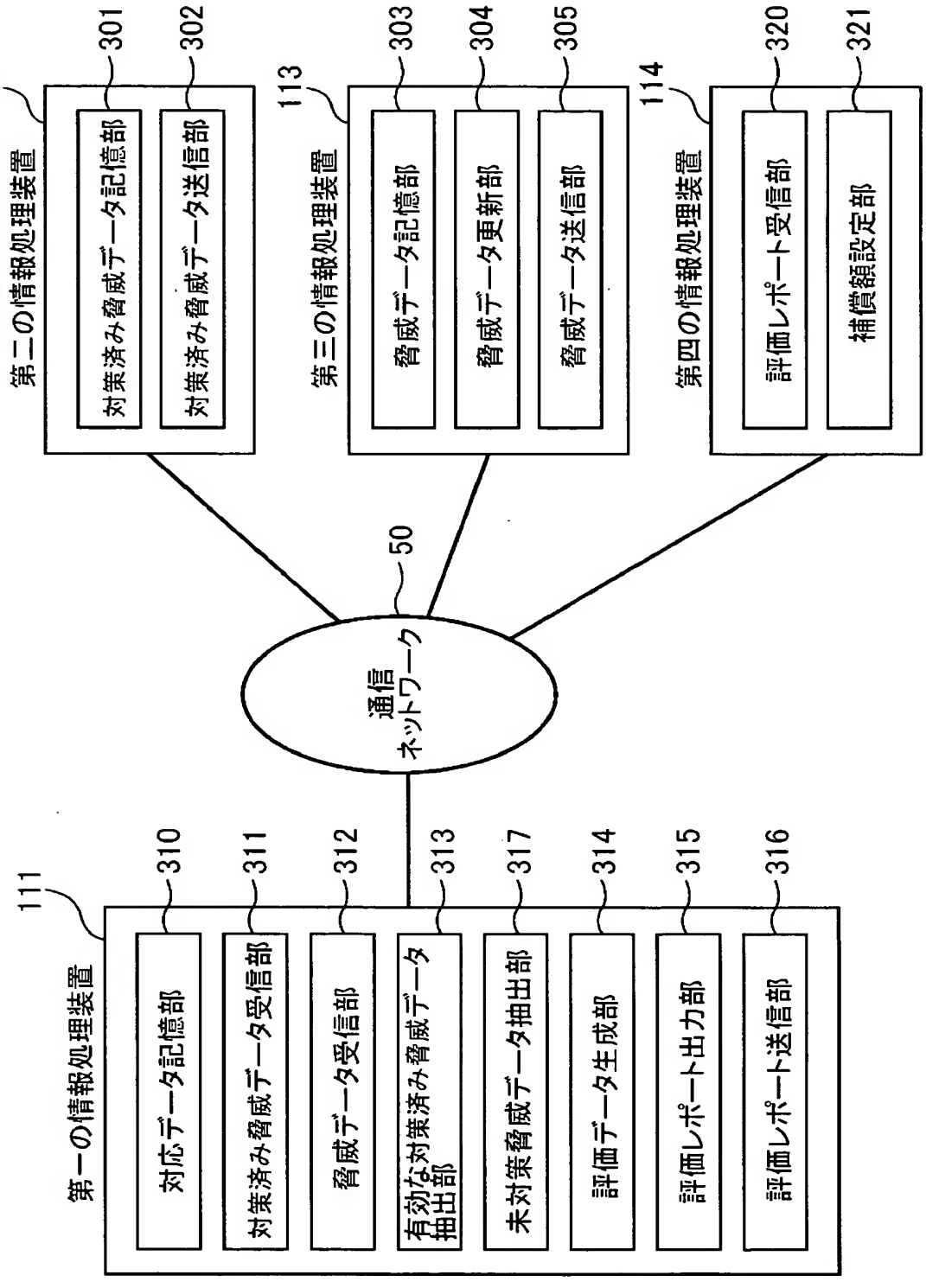
【図９】


第一のサイト
101
第二のサイト
102
第三のサイト
103
111
112
113
第一の情報処理装置
第二の情報処理装置
第三の情報処理装置
S912
対策済み脅威データを受信
S911
対策済み脅威データ管理テーブルを送信
S914
脅威データを受信
S913
脅威データ管理テーブルを送信
S915
有効な対策済み脅威データを抽出
S916
未対策の脅威データを抽出
S917
評価データ生成
S918
評価レポート生成
S919
評価レポート送信

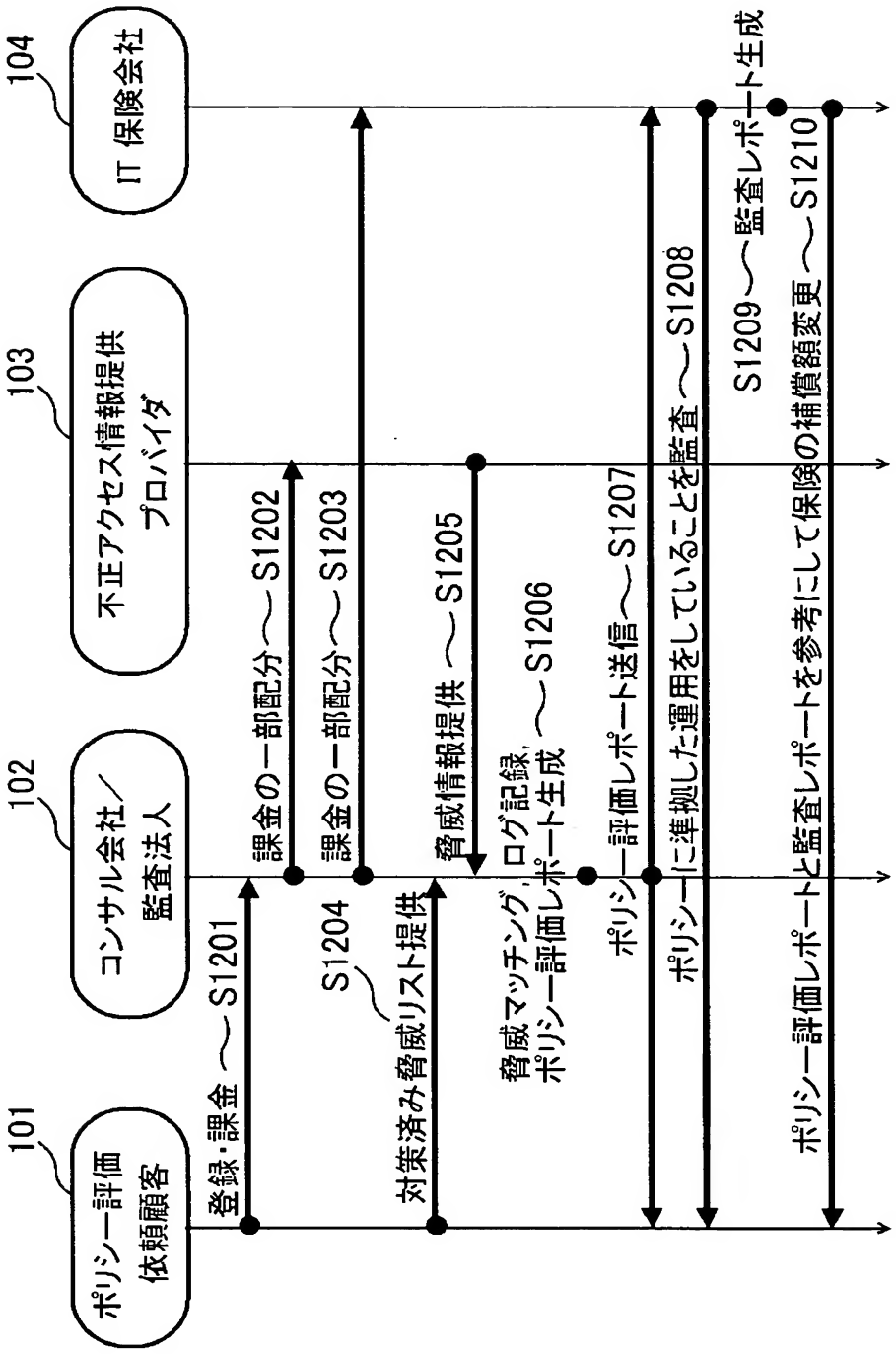
【図１０】


第一のサイト
(コンサル会社/監査法人)
第一の情報処理装置
(ポリシー監査・管理装置)
111
101
第二のサイト
(ポリシー評価依頼顧客)
第二の情報処理装置
(ポリシーデータ装置)
112
102
第三のサイト
(不正アクセス情報提供プロバイダ)
第三の情報処理装置
(情報提供装置)
113
103
第四のサイト
(IT保険会社)
第四の情報処理装置
(補償額設定装置)
114
104
通信
ネットワーク
50

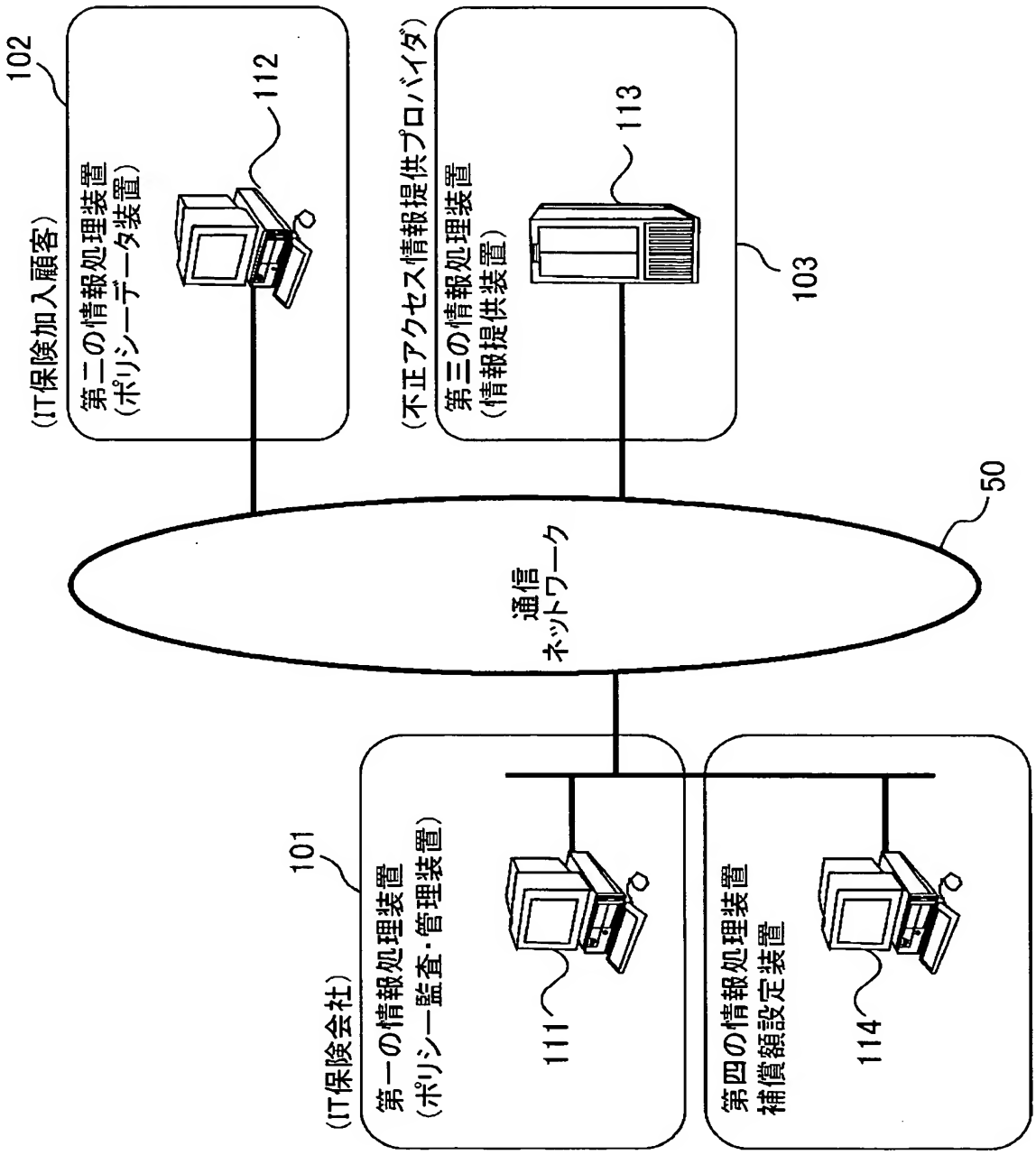
【図１１】


第一の情報処理装置
111
対応データ記憶部
310
対策済み脅威データ受信部
311
脅威データ受信部
312
有効な対策済み脅威データ抽出部
313
未対策脅威データ抽出部
317
評価データ生成部
314
評価レポート出力部
315
評価レポート送信部
316
通信ネットワーク
50
第二の情報処理装置
112
対策済み脅威データ記憶部
301
対策済み脅威データ送信部
302
第三の情報処理装置
113
脅威データ記憶部
303
脅威データ更新部
304
脅威データ送信部
305
第四の情報処理装置
114
評価レポート受信部
320
補償額設定部
321

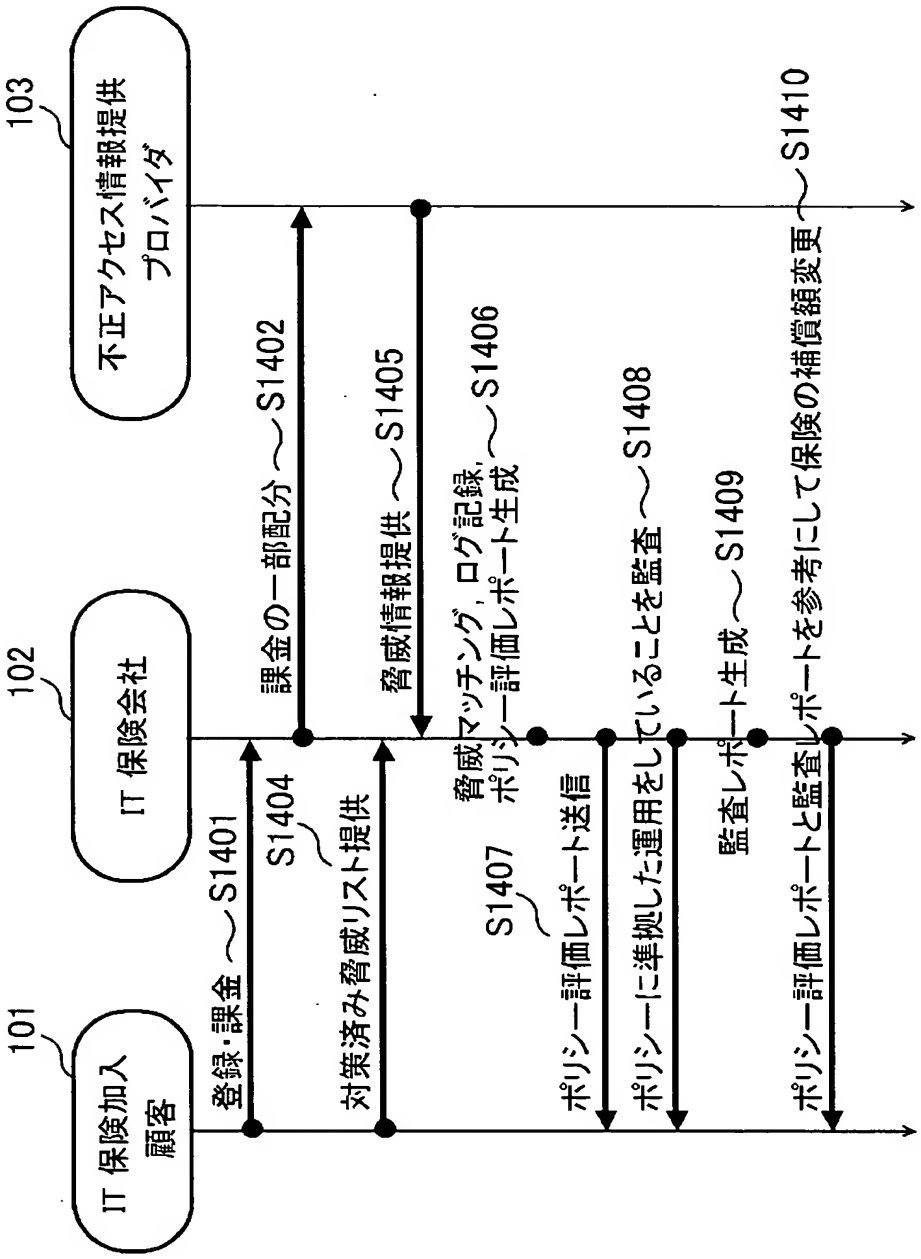
【図１２】


101
ポリシー評価
依頼顧客
102
コンサル会社／
監査法人
103
不正アクセス情報提供
プロバイダ
104
IT 保険会社
登録・課金 ～S1201
課金の一部配分 ～S1202
課金の一部配分 ～S1203
S1204
対策済み脅威リスト提供
脅威情報提供 ～S1205
脅威マッチング，ログ記録，
ポリシー評価レポート生成 ～S1206
ポリシー評価レポート送信 ～S1207
ポリシーに準拠した運用をしていることを監査 ～S1208
S1209～監査レポート生成
ポリシー評価レポートと監査レポートを参考にして保険の補償額変更 ～S1210

【図１３】


102
(IT保険加入顧客)
第二の情報処理装置
(ポリシーデータ装置)
112
(不正アクセス情報提供プログラム)
第三の情報処理装置
(情報提供装置)
113
103
50
通信
ネットワーク
101
(IT保険会社)
第一の情報処理装置
(ポリシー監査・管理装置)
111
第四の情報処理装置
補償額設定装置
114

【図１４】


101
IT 保険加入顧客
102
IT 保険会社
103
不正アクセス情報提供プロバイダ
登録・課金 ～S1401
課金の一部配分 ～S1402
S1404
対策済み脅威リスト提供
脅威情報提供 ～S1405
S1407
脅威マッチング，ログ記録，ポリシー評価レポート生成 ～S1406
ポリシー評価レポート送信
ポリシーに準拠した運用をしていることを監査 ～S1408
監査レポート生成 ～S1409
ポリシー評価レポートと監査レポートを参考にして保険の補償額変更 ～S1410

【書類名】要約書
【要約】
【課題】企業等の組織において情報セキュリティポリシーを効率よくかつ適切に策定し運用することができる情報セキュリティポリシー評価システムを提供する。
【解決手段】
第二のサイト１０２の第二の情報処理装置１１２から第一のサイト１０１の第一の情報処理装置１１１に第二のサイト１０２で運用されている対策済み脅威を送信し、脅威に関する情報を収集している第三のサイト１０３から第一のサイト１０１の第一の情報処理装置１１１に脅威情報を送信し、第一の情報処理装置１１１は、受信した対策済み脅威のうち実際に生じた脅威に対して有効であった対策済み脅威や未対策の脅威を抽出し、それらを記載した評価レポートを生成する。また生成された評価レポートに基づいて、脅威に対する保険の補償額を変更する。
【選択図】　図１

特願２００３－３４３４８０

# 出　願　人　履　歴　情　報

識別番号　［０００００５１０８］

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所